hakin9

GSM

Qui peut écouter mon portable?

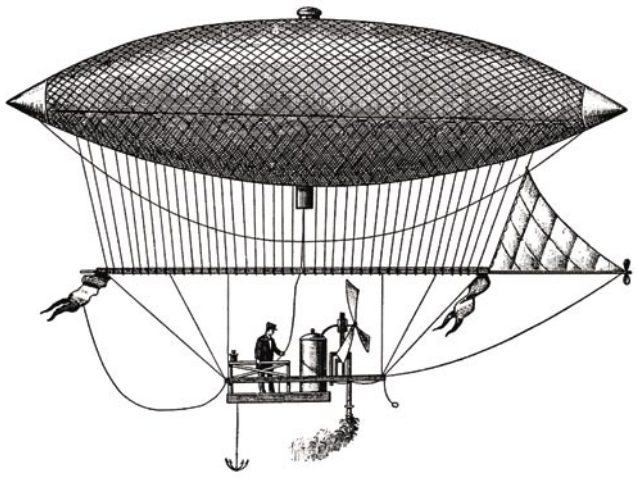
Reinhard Wobst

Article publié dans le numéro 1/2004 du magazine "Hakin9".

Magazine "Hakin9", Wydawnictwo Software, ul. Lewartowskiego 6, 00-190 Warszawa, piotr@software.com.pl

Qui peut écouter mon téléphone mobile ?

Reinhard Wobst



Cet article traite de la sécurité des téléphones mobiles dans le sens général. Est-ce possible d'écouter votre conversation ? Quels appareils sont nécessaires pour cela ? Une personne malintentionnée peut-elle se servir de votre numéro de téléphone ? Quelles données privées peuvent être révélées pendant l'utilisation d'un téléphone mobile ?

Les téléphones mobiles basés sur le standard GSM (appelé aussi téléphones numériques cellulaires) sont utilisés par environ 800 millions de personnes dans le monde (ce nombre augmente très vite et peut être bientôt dépassé). Presque chaque téléphone mobile ordinaire que vous pouvez trouver dans l'Europe de l'Est ou d'Ouest est basé sur ce standard. Alors, chaque trou de sécurité dans ces téléphones est critique car il est très difficile à réparer : les algorithmes et les protocoles sont assignés au matériel et, de cela, il est impossible de mettre à jour un billion d'appareils téléphoniques (c'est-à-dire : échanger) comme un programme de sécurité quelconque. Nous pouvons croire que l'algorithme de chiffrement A5 – qui est utilisé pour chiffrer le trafic radio dans les téléphones GSM – est un algorithme de chiffrement le plus utilisé dans le monde. Une faille de sécurité dans cet algorithme peut être lourde de conséquences.

Est-ce vrai ? A5 *est* faible ! Mais pas de panique, il n'est pas du tout facile d'écouter vos conversations téléphoniques par les amateurs. Au moins, pas dans les cinq prochaines années.

La sécurité ne signifie pas seulement de rendre difficile l'écoute de nos conversations. L'authentification est aussi importante, comme la preuve d'identité. Si cela n'est pas sûr, les autres peuvent téléphoner à vos frais. Mais y peuvent-ils ? Oui, ils peuvent bien ! Mais ce n'est pas si facile que ça et vous pouvez le prévenir.

Enfin, votre téléphone peut être localisé. Cela signifie que votre fournisseur de services mobiles peut localiser votre téléphone avec, théoriquement, une assez grande précision. Cette possibilité résulte de la topologie du réseau. Ce n'est pas question de sécurité dans le sens plein du mot. Pourtant, du point

Auteur

L'auteur étudiait les mathématiques et il a soutenu sa thèse de doctorat en processus stochastiques. Maintenant, il s'occupe de la cryptographie, de la sécurité des données et de la programmation en C/C++ et en langages script sous UNIX. Il crée les programmes scientifiques et industriels et est connu comme auteur de plus de 150 articles et livres sur la cryptologie.

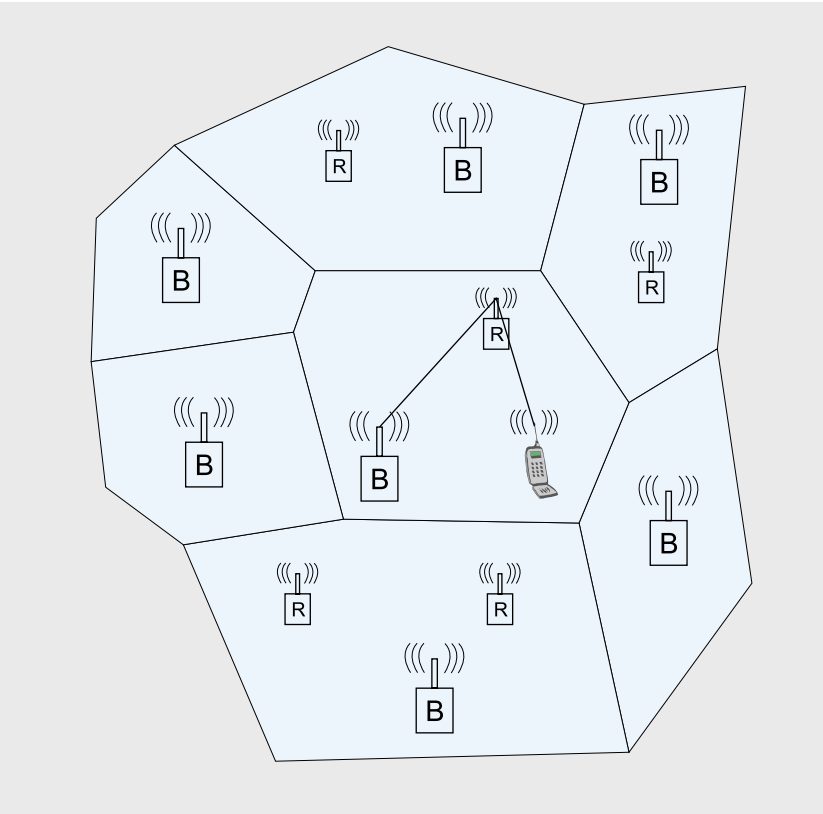


Figure 1. *Dans chaque cellule, vous pouvez trouver exactement une station de base (B), éventuellement les répéteurs (R) – et, quelque part, des téléphones*

de vue de votre sécurité, il est très important avec quelle précision la localisation est effectuée et, avant tout, qui se servira de cette information. Vous ne pouvez rien changer mais vous devez connaître différents trucs et astuces. La localisation est l'une des plusieurs possibilités offertes par l'âge de l'information à venir.

Alors, ne vous attendez pas à pouvoir pirater les téléphones GSM après avoir lu cet article. Les personnes qui travaillent dans les services secrets peuvent vous fournir des moyens nécessaires, mais je crois qu'elles ne sont pas autorisées à le faire. Pourtant, vous comprendrez mieux comment les téléphones GSM fonctionnent et quels dangers sont réels ou seulement hypothétiques.

Comment fonctionne le système GSM ?

GSM est un standard très complexe. La documentation respective compte plus de 7000 pages. Le principe de base présenté sur la figure 1 est probablement bien connu : le réseau constitué des postes appelés stations de base divise le territoire en cellules virtuelles ; une seule station de base se connecte à tous les téléphones mobiles à l'intérieur de la cellule. Dans les vallées, grands bâtiments, voies sousterraines, etc., vous trouverez souvent les répéteurs. Ce sont des stations relais et aident à réémettre le signal reçu plus loin.

Théoriquement, chaque station de base peut recevoir et émettre simultanément sur environ 140 canaux. C'est une limite technique. La bande de fréquences pour les téléphones GSM est déterminée dans la spécification, les fréquences des cellules adjacentes sont différentes et chaque canal doit disposer d'une bande passante minimale. En pratique, on utilise moins de canaux. Mais vous comprenez pourquoi les cellules dans les villes combles sont petites – parfois, elles ont le diamètre d'environ 100 mètres – et peuvent être très grandes (d'environ 20 km) dans les endroits ruraux. Un exemple extrême d'une cellule est la foire CeBIT à Hannover où sur une surface de quelques kilomètres carrés le nombre de téléphones utilisés simultanément est comparable à celui utilisé dans une ville d'un million d'habitants comme Colonia.

Les explications sont encore insuffisantes. Chaque canal est divisé en huit sous-canaux suivant le temps partagé. Cela signifie que huit téléphones peuvent utiliser la même fréquence ; la station de base affecte un intervalle de temps à chaque téléphone. Chaque intervalle dure 4.6 millisecondes. Théoriquement, environ 1000 personnes peuvent téléphoner dans une cellule de la base en même temps.

Et ce n'est pas toutes les complications : la fréquence peut changer pendant la communication ce qui est appelé *saut de fréquence*. Cela rend le travail des pirates plus difficile et, en même temps, a une application pratique. Si les ondes radio sont brouillées par certaines obstacles (comme un pont ou un bâtiment en verre et acier), une autre fréquence peut mieux convenir. Le système entier est constamment optimisé – la puissance du signal de votre téléphone est ajustée à la qualité de réception de la station de base ou d'un répéteur, la fréquence change et même la station de base et le débit peuvent changer. Vous comprenez maintenant qu'il n'est pas possible de capturer le trafic radio à l'aide des dispositifs amateurs.

Authentication

Nous avons vu approximativement comment fonctionne l'interface radio. Et quant au traitement des données ? Votre voix est numérisée, compressée de façon très efficace, chiffrée et envoyée en paquets de 114 bits chacun. Avant cela, les deux parties (le téléphone et la station de base) doivent déterminer une clé de chiffrement, de plus l'authentification de votre téléphone est effectuée. Le

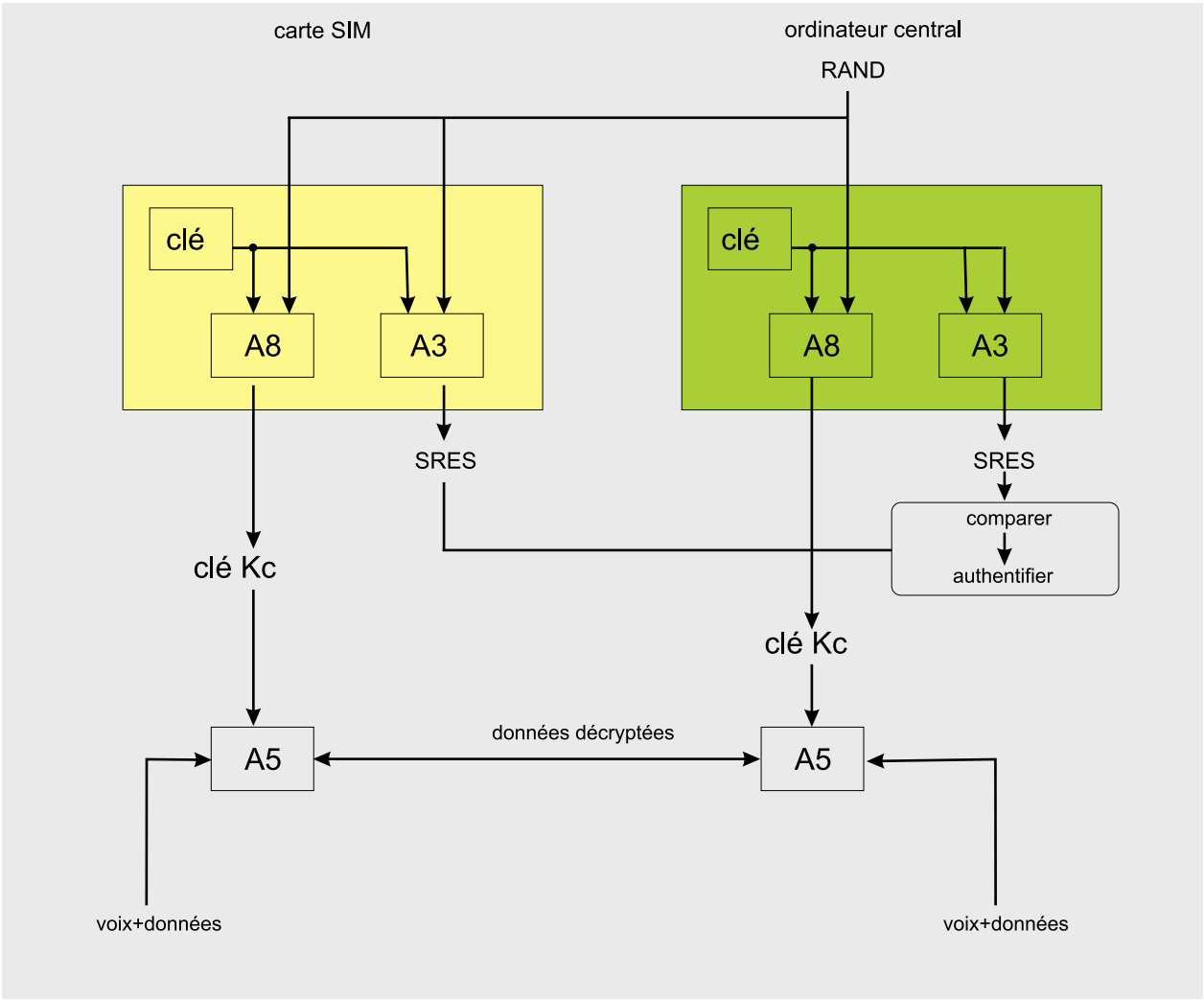


Figure 2. *L'authentification et la génération de la clé (voir les explications dans le texte)*

processus entier est présenté sur la Figure 2.

Un élément critique de la sécurité est votre petite carte SIM. Le téléphone seul n'est qu'un type de fournisseur de services (afficheur, clavier, interface radio...). Votre carte SIM possède un numéro de série unique et une clé secrète de 64 bits gravés. De plus, deux algorithmes cryptographiques ont été implémentés : A3 et A8. Le numéro de série est votre vrai numéro de téléphone. Votre fournisseur le transcrit de façon logique en numéro pouvant être lu par les humains (pourtant, vous pouvez garder votre numéro quand vous changer votre carte SIM). La relation est similaire à celle entre les numéros inode et les noms des fichiers sous UNIX/Linux. Aussi la protection via PIN constitue un petit ordinateur à l'intérieur de la carte SIM.

La clé secrète est physiquement protégée contre la lecture de l'extérieur. Je ne sais pas quelles astuces ont été utilisées pour atteindre ce but (et elles peuvent changer), mais elle est conçu de façon très robuste. Probablement, il faudrait détruire la carte SIM pour extraire directement la clé secrète.

Cette clé secrète est la base du système de protection GSM. Vous l'obtenez de votre fournisseur avec la carte au moment où vous l'achetez. Votre fournisseur sauvegarde aussi les clés sur les disques durs de ses ordinateurs et j'espère qu'elles sont bien protégées. Les cartes SIM sont un simple moyen de distribution des clés. La clé de chiffrement publique (voir [5]) pourrait être trop lente, trop chère et inutile dans notre cas.

Quand vous allumez votre téléphone, celui-ci envoie le numéro de série de votre carte vers la station de base la plus proche. Cette station de base l'envoie ensuite vers les ordinateurs centraux de votre fournisseur qui connaît le numéro de la clé secrète correspondant et vous renvoie un numéro aléatoire RAND.

Votre carte SIM calcule la signature SRES = A8(RAND, clé) et l'envoie vers la station de base. Entre temps, la station de base reçoit SRES de la part des ordinateurs centraux. Si le résultat est conforme à votre SRES, vous êtes authentifiés. Vous devez seulement connaître la clé, outre le fournisseur lui-même. Celui qui ne connaît pas

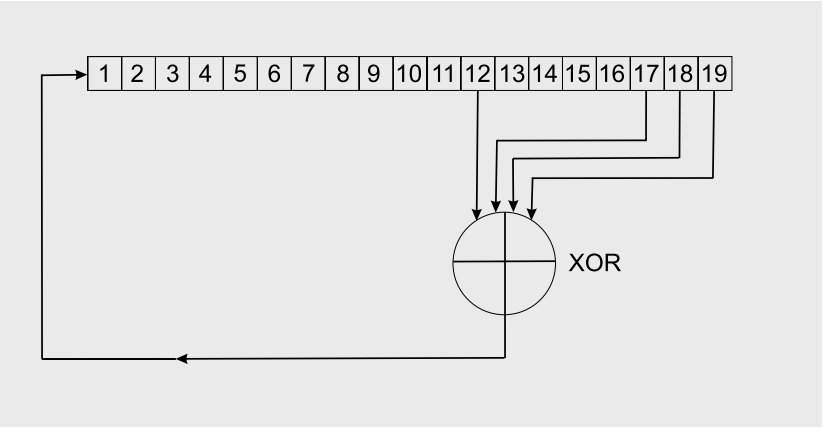


Figure 3. *Algorithme de chiffrement A5*

la clé, ne sera pas capable de calculer SRES.

En même temps, votre carte SIM et les ordinateurs centraux calculent aussi la clé de chiffrement Kc = A3(RAND, clé). C'est un numéro codé sur 64 bits qui sert comme code de déchiffrement. La clé Kc est envoyée ensemble avec SRES vers la station de base.

Désormais, toute la communication est déchiffrée par l'algorithme A5 (qui est implémenté dans l'appareil téléphonique pour raison de performance), à l'aide de la clé Kc.

Aspects de la sécurité

Vous voyez – comme dans le chiffrement de la clé publique, aucune information secrète n'est transférée en texte clair sur le canal radio non sécurisé et votre clé secrète ne quitte même pas les ordinateurs centraux du fournisseur. Et qu'est-ce qui se passe dans le cas où vous appelez de l'étranger, au sein des réseaux des fournisseurs étrangers qui ne connaissent pas votre clé secrète ?

Si vous allumez votre téléphone dans le réseau d'une société qui a le contrat de roaming avec votre fournisseur, ce réseau reconnaît à qui le téléphone appartient et demande le triplet approprié [RAND, A3(RAND, clé), A8(RAND, clé)] dans votre pays d'origine. Cela explique pourquoi la première connexion à un réseau étranger peut durer quelque temps et la seconde fois, elle est si rapide comme une connexion ordinaire (si le réseau étranger n'a plus de triplets, de nouveaux numéros sont requis à temps). Remarquez : encore une fois votre clé secrète n'est pas révélée, même au fournisseur de confiance.

Nous avons montré que A3, A8 et A5 sont sûrs, alors tout le système est presque sûr. Il n'existe que quelques points faibles :

- Votre téléphone est authentifié dans votre station de base, mais pas inversement. Le téléphone n'est pas capable de notifier qu'il se connecte à une fausse station de base. Pour cela, on utilise le numéro d'abonné IMSI (voir dan sla suite de l'article). Cette fausse station de base ne connaît pas votre clé mais elle peut extraire les informations de la phase initiale de la conversation et contraindre votre téléphone à faire des choses que vous ne voulez pas, p. ex. désactiver le chiffrement.
- Les paquets de données n'ont pas de sommes de contrôle cryptographiquement fortes. Le numéro d'abonné IMSI peut les falsifier (nous allons en parler dans la suite) et renvoyer vers la station de base. C'est l'attaque man-in-the-middle typique.
- Les paquets de données possèdent des numéros de séquences non protégés. Cela permet à l'attaquant de renvoyer vos paquets encore une fois (on ne sait pas pourquoi).

Algorithme de chiffrement A5

La figure présente le registre LSFR (en anglais *linear feedback shift register*) qui se traduit en français comme registre à décalage à rétroaction linéaire dont la longueur est de 19 bits. Au début, ce registre a une clé (dans cette exemple, elle est longue de 19 bits). Le déchiffrement d'un bit se fait comme suit : dans la boucle, les bits 12, 17, 18 et 19 sont soumis à l'opération or exclusif et le résultat est mis dans le bit de position 1 après tous les bits 1...18 qui ont été déplacés d'une position vers la droite. L'un peut utiliser ce produit XOR de quatre bits, appelé rétroaction, comme bit-clé ou bit supérieur. Cette clé-bit est soumise à l'opération XOR avec un bit de texte, et en résultat, on obtient le bit chiffré. Toute cette procédure est ensuite répétée pour le bit de texte suivant, et ainsi de suite.

La sécurité dépend de la longueur du registre et des positions du bit qui est appelée séquence de dérivation (en anglais : *tap sequence).* Mais un simple chiffrement LSFR est assez faible (les informations plus détaillées sont disponibles dans [13]). Les algorithmes modernes utilisent les *nonlinéarités*. Dans le cas de l'algorithme A5, nous avons trois LFSRs de longueur 19, 22 et 23 bits (ensemble, il constituent la clé de 64 bits) avec différentes séquences de dérivation. A la sortie, on obtient le produit XOR des bits moyens, p. ex. ceux des positions 10, 12 et 12. Le bit de seuil est mis à 1, si au moins un bit moyen est mis, autrement, il est mis à 0. Chacun de ces trois LFSR est traité, si son bit moyen est différent du bit de seuil. C'est de la non-linéarité et tout cela constitue justement l'algorithme A5 (le mélange initial n'a pas été décrit dans cet article).

Évidemment, cet algorithme est bon dans le cas des appareils, et de plus, fonctionne très rapidement dans vos téléphones. – Vous pouvez aussi trouver une simple implémentation en C dans la *bible* [13] de Schneier ou sur le CD disponible sur le Web [5].

Comment cracker l'authentification ?

L'attitude *sécurité par obscurité*, p. ex. laisser les algorithmes en cachette, n'a jamais été utile pour la sécurité (outre quelques services secrets expérimentés comme NSA). C'était le destin des algorithmes A3 et A8. Ils n'étaient jamais publiés dans les spécifications GSM ni rendus public. Évidemment, les algorithmes très fréquemment utilisés ne pouvaient pas rester trop longtemps secrets, et enfin, ils ont été révélés. À présent, les jeunes cryptologistes Goldberg et Wagner de Berkeley ont eu besoin d'un seul jour (notamment April 13th, 1998) pour y trouver des faiblesses [1]. Ils soulignaient que leur approche n'était pas si novatrice et que chaque bon cryptanalyste pourrait trouver des trous de sécurité.

L'attaque de Goldberg et Wagner exigeait accès à la carte SIM qui, quant à elle, reçoit les arguments d'entrée RAND. En fonction des réponses SRES obtenues, les numéros RAND ont été envoyés de nouveau, et ainsi de suite. Après environ 150.000 cycles similaires, la clé secrète a été révélée et toute la sécurité du téléphone s'en est allée. Le pirate est capable d'émuler la carte SIM à l'aide d'un ordinateur PC connecté à un téléphone quelconque et peut utiliser votre téléphone pour appeler les lignes roses surtaxées. Ou bien, commander 50 pizzas et 74 livres de Harry Potter qui seront livrés chez vous. Ou encore, faire quelques méchants appels téléphoniques à votre nom. L'attaque décrite fonctionne en pratique ce qui a été montré par German Chaos Computer Club.

Est-ce vraiment si facile ? Non. La carte SIM n'est pas un superordinateur et pour effectuer environ 150.000 appels, il faut à peu près 8 heures. L'attaquant doit prendre votre téléphone pendant ce temps sans que vous vous en rendiez compte (mais vous pouvez appeler votre fournisseur pour dé r votre mobile). L'obstacle suivant est le code PIN. Il a seulement de 4 jusqu'à 8 chiffres, mais après 3 échecs, la carte SIM est arrêtée, et vous devez entrer le code Super PIN. Si celui-ci est erroné, après le 10ème essai, la carte est désactivée. Mais en pratique, c'est encore pire. Si vous louez une voiture, vous prenez parfois aussi le téléphone avec ou même sans code PIN. Alors là, c'est une belle occasion pour les attaquants professionnels !

L'attaque la plus dangereuse mais plutôt théorique peut être effectuée par voie aérienne en envoyant les requêtes aux téléphones allumés. Pour cela, vous avez besoin d'un équipement spécial (similaire à IMSI- catcher). Vous devez aussi avoir beaucoup de temps et un abonné qui ne réfléchit pas trop pourquoi son téléphone est tout le temps en marche et consomme de l'énergie, jour après jour.

Enfin, la combinaison A3/A8 étudiée (appelée aussi COMP128)

Qu'est-ce que c'est qu'un capteur IMSI ?

IMSI se traduit comme *International Mobile Subscriber Identity* et c'est simplement le numéro de série de votre téléphone, ce qui a été déjà mentionné dans cet article. D'autre part, l'IMSI-catcher n'est pas un équipement d'espionnage typique, malgré son nom. Il est utilisé pour effectuer les mesures et plutôt inoffensif sans l'antenne externe. Les ingénieurs s'en servent pour simuler la station de base afin de tester les téléphones mobiles. À présent, vous pouvez acheter ces appareils aux dimensions d'une valise chez Rohde & Schwarz au prix de 10000 EUR. En tant qu' appareil de mesure, il peut être exporté. Cet IMSI-catcher connaît la plupart (ou bien tous) des protocoles GSM, ainsi que l'interface radio, y compris les bonds de fréquence.

Pourtant, il peut être utilisé de façon impropre, s'il est équipé d'un amplificateur et d'une antenne. Alors, il peut devenir une station de base pour tous les téléphones mobiles dans un rayon de 300m, et il peut devenir un téléphone pour une station de base successive. Dans la cryptographie, ces attaques sont appelées attaques *man-in-the-middle*.

La première possibilité : en donnant le numéro d'un téléphone quelconque à ce dispositif, vous êtes capables de capturer les numéros IMSI de tous les téléphones dans le voisinage. Cela exige une intervention active parce que normalement, pour des raisons de sécurité, les téléphones utilisent l'identité temporaire appelée TMSI (Temporary Mobile Subscriber Identities). Alors, la police qui se sert d'IMSI-catcher peut savoir qui a le téléphone allumé dans le voisinage, sans qu'il soit suspect ou pas (pour se faire, elle doit connaître la relation entre IMSI et le numéro de téléphone). Évidemment, une telle utilisation peut troubler de façon importante le trafic GSM, et beaucoup de personnes non concernées peuvent être observées. Officiellement, en Allemagne cet usage est interdit (mais probablement pratiqué malgré tout).

L'autre possibilité envisagée dans l'article consiste à forcer les téléphones à utiliser le chiffrement faible A5/2 à la place de A5/1. Il est également possible de désactiver totalement le chiffrement. Un de mes amis, plusieurs fois a vu un point d'exclamation sur l'afficheur d'un téléphone Siemens. Conformément à la documentation, cela signifie que le chiffrement a été désactivé. Un expert a été très étonné quand il a appris ça. Nous ne savons pas exactement qu'est-ce qui s'est passé en réalité, mais nous vous conseillons de rester vigilant en voyant des choses pareilles.

Certes, les IMSI-catchers peuvent être aussi utilisés pour l'écoute passive. Cela a du sens, si vous pouvez cracker A5/1 comme décrit dans l'article. Nous pouvez deviner que les personnes ingénieuses sont capables de construire des dispositifs moins chers pour l'écoute passive. Enfin, officiellement, vous ne pouvez pas les acheter. Et si quelqu'un apprend que vous possédez un IMSI-catcher, vous pouvez avoir des problèmes pour expliquer pourquoi vous en avez besoin.

A propos, il y a quelques années, on disait que les gars de NSA ont eu les cartes PCMCIA qui permettaient d'écouter tous les numéros de téléphones réels dans les environs. Probablement, ce n'était pas pour les téléphones GSM, mais je parie qu'ils l'ont déjà.

n'est qu'une proposition. La question de modification de ces algorithmes dépend des fournisseurs. En Allemagne, seul Mannesmann (maintenant Vodafone D2) utilisait la forme originale. Pourtant, j'ai des doutes que les autres algorithmes, encore plus secrets soient plus sûrs. On dit que l'industrie a élaboré son successeur, COMP128-2. Mais il n'est pas encore publié.

Cette attaque a produit un effet secondaire très intéressant. Notamment, dans toutes les cartes SIM testées, le code de déchiffrage Kc généré n'était long que de 54 bits, et pas de 64. Cette réduction a été expliquée par les fournisseurs comme *une réaction plus souple aux dangers liés à la sécurité.* Il serait très intéressant de savoir quoi ou qui a causé cette réduction de la longueur de la clé. Probablement, nous n'obtiendront aucune réponse. En tout cas, ce n'est pas tellement important – veuillez bien lire le paragraphe suivant.

Comment cracker le chiffrage ?

Pour éviter des malentendus : seul le trafic au travers un canal radio est crypté parce que, théoriquement, chacun, équipé d'un IMSI-catcher peut l'écouter. Le trafic entre la station de base et les passerelles au réseau téléphonique câblé n'est pas chiffré. Au moment où les connexions sont de préférences réalisées par câbles en fibre optique, il est plus difficile de faire l'écoute. Bien sûr, pour les amateurs. Toutes les agences de sécurité de votre pays ont certainement accès à ces connexions. En Allemagne, cela est exigé par la loi. L'accès doit être anonyme (p. ex. le fournisseur ne doit pas savoir quand ni quoi est écouté). C'est étrange, mais cette possibilité a été complètement oublié au moment où les téléphones cellulaires ont été introduits sur le marché au début des années 90. Les mises à jour ont coûté dizaines de millions de marks que les fournisseurs ont dû payer.

L'algorithme de déchiffrement A5 (plus précisément A5/1) est présenté sur la figure 3. Il est aussi appelé chiffrement de flux : la trame de bits dépendante de la clé est générée indépendamment du texte en clair (p. ex. les données qui doivent être chiffrées), et soumise à l'opération xor. Le destinataire doit faire de même pour obtenir de nouveau du texte en clair. Pourtant, si un pirate change un bit dans le flot de données chiffrées en chemin vers la station de base, le même bit sera changé après le déchiffrement. C'est pourquoi, les chiffres continus doivent être utilisés ensemble avec les sommes de contrôle sécurisées. Ce n'est pas une solution pour GSM. Alors, l'attaquant avec un IMSI-catcher et assez intelligent est capable de modifier vos données... s'il sait où modifier. C'est un danger potentiel pour la transmission des données, mais pas pour les appels vocaux.

Cracker A5 directement

Les deux (!) algorithmes A5 restaient secrets et ils furent révélés en 1994 ; le projet entier fut reconstitué en 1999 par Briceno.

Les cryptoanalystes sont d'accord que A5 est faible bien qu'aucune attaque pratique ne soit pas encore connue (parfois vous savez par expérience et du projet même qu'un algorithme n'est pas sûr, mais vous ne savez pas exactement comment s'y attaquer). On disait que l'Allemagne s'obstinait à un algorithme fort (parce que la situation avait lieu pendant la phase de planification – en 1988 – directement derrière le rideau de fer), pendant que la France voulait un algorithme faible. La France a longtemps interdit l'usage général de la cryptographie forte et l'avait soumise au contrôle des exportations face aux pays avec beaucoup d'argent et beaucoup de pétrole. Si c'était comme ça, la France en gagnerait et nous aurions perdus.

Il y a dix ans, c'était encore dangereux de parler de ces choses-là. Dr Shepherd de l'Université de Bradford voulait présenter la cryptoanalyse de l'algorithme A5 pendant le colloque d'IEEE à Londres, le 3 Juin 1994, mais son cours a été arrêté à la dernière minute (qui l'a arrêté ? et comment ? Je n'en sais rien).

Maintenant, la situation est différente. En 2000, deux célèbres cryptoanalystes Biryukov et Shamir ont craqué A5 de façon très étonnante. Pour ce faire, vous avez besoin d'un PC avec deux disques durs de 73 Go chacun – dans cinq ans, votre frigo les aura par défaut – remplis de certaines données (un mathématicien qualifié peut vous aider à les générer). Ensuite, vous avez besoin d'une sortie d'A5/1 pour deux minutes et une seconde (!) pour les calculs. Et voilà, vous avez la clé et vous pouvez écouter les conversations. Lisez ce fragment très attentivement : la sortie d'A5/1, et pas le texte chiffré. Autrement dit : vous avez besoin du texte en clair, ainsi que du texte chiffré intercepté. Ce n'est pas une attaque pratique, elle n'est même pas dangereuse pour la transmission des données (cette déclaration dans mon livre [3,5.7.2], est fausse – elle a été corrigé sur la page de l'errata). La solution alternative peut être de *deux secondes pour les données, quelques minutes pour les calculs*. Je ne sais pas si cela pourrait être utilisé pour les attaques pratiques. Les auteurs ne se plaignent pas ouvertement de la sécurité GSM.

Dans l'attaque, même les 10 bits ne sont pas utilisés. Les détails sont présenté dans [3], mais vous devez avoir une compréhension mathématique pour tout comprendre. Et comme c'est dans les habitudes des cryptoanalystes – aucun programmes n'est accessible.

A5/2 – joie de l'attaquant

Évidemment, dans les années '90, les politiciens avaient encore peur que A5 pourrait devenir trop fort et aider les terroristes et criminels. De cela, dans presque tous les téléphones, on a implémenté une version d'exportation d'A5 appelée A5/2 (pourtant, l'algorithme complet A5

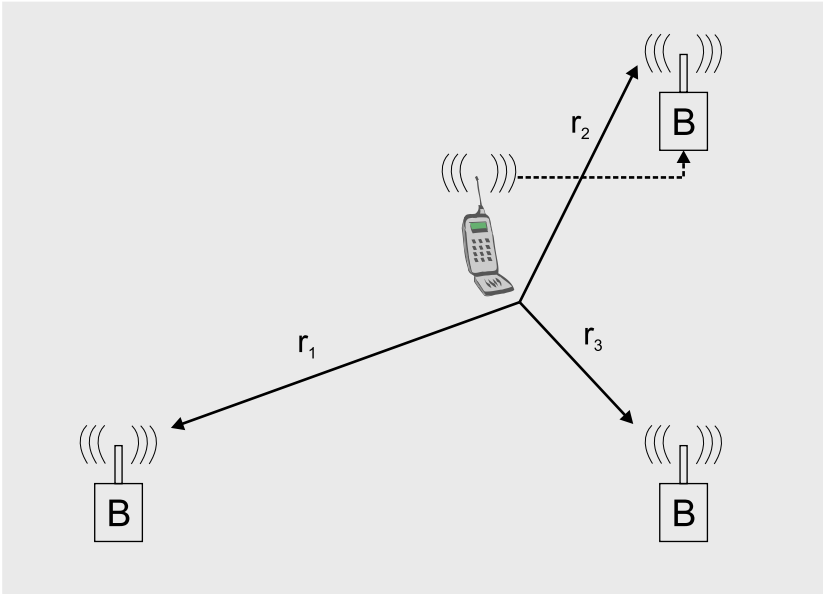


Figure 4. *La localisation par mesurage des différences de la durée du signal dans une station de base ; le résultat est envoyé dans la station de base suivante*

est également appelé A5/1). Une nouvelle attaque révélée en 2003 [4] a une référence pratique. Les auteurs ont profité du fait que les codes de correction des erreurs ont été ajoutés aux paquets de données et tous cryptés ensemble. C'est une sorte de dépendance algébrique à l'intérieur d'un texte chiffré et peut être utilisée pour effectuer une attaque triviale. Quelques dizaines de milisecondes d'écoute d'une communication cryptée et une seconde de calculs suffisent pour le décryptage. Ce dont vous avez besoin, c'est un IMSI-catcher placé près du téléphone qui simule une station de base. Cet IMSI-catcher exige de passer de l'algorithme de chiffrement A5/1 à A5/2. Et ensuite, il écoute et envoie toutes les données à un PC quelconque. Vous pouvez lire les informations plus détaillées dans [4]. Et encore, une connaissance mathématique est nécessaire pour comprendre les informations de cet article. Il ne présente pas un programme tout prêt, mais vous y trouverez assez d'informations pour l'écrire vous-mêmes. Il est très drôle de lire dans l'article : *Les méthodes et les idées (...) sont brevetées, et leur utilisation sans l'autorisation écrite est interdite.* Alors, chers detectives privés, organes de polices et services secrets : veuillez bien acheter une licence !

Qu'est-ce qui est nécessaire pour écouter ?

Comme vous avez pu voir, le piratage d'un réseau WLAN est un jeu d'enfant en comparaison avec le branchement clandestin au réseau GSM. Probablement, un IMSI-catcher modifié est une première condition pour le faire (cf. l'encadré). C'est pourquoi, vous avez besoin de personnes qui connaissent la cryptoanalyse aussi bien que la structure de GSM et qui sont capables d'implémenter l'algorithme A5/2 dans un programme. Alors, votre voisin ne peut pas écouter vos appels, à moins qu'il n'ait accès à l'argent, aux dispositifs nécessaires et aux personnes qualifiées. Je vous conseille de baisser les jalousies en fermant toutes vos fenêtres pendant que vous parlez des affaires importantes – les microphones laser sont moins chers et il est plus facile de les acquérir.

Ne vous préoccupez pas de la police. Elle peut recevoir tout le trafic déchiffré de façon beaucoup plus confortable directement du fournisseur, comme je l'ai déjà mentionné. Son appétit de données est énorme et augmente constamment, toujours plus grande que celle d'un citoyen ordinaire. Le nouveau nom officiel pour cet appétit faim est maintenant *lutte contre le terrorisme*. Le chiffrement aérien est une protection contre les petits services secrets étrangers et les detectives manqués. Dans les années qui viendront, la base technique sera de plus en plus développée et j'espère que le protocole UMTS aura une chance de passer dans l'usage général.

Services basés sur la localisation

Quand nous parlons de l'appétit de données du côté des organes de pouvoir public, il ne faut jamais oublier que ce n'est pas seulement le contenu des appels téléphoniques qui est important. L'analyse de trafic offre beaucoup plus de données qu'on ne se rend pas compte. *L'analyse de trafic* signifie : quand vous avez téléphoné, combien de temps cela vous a pris et qui a été votre destinataire ? Cela signifie aussi : qui vous a envoyé des e-mails ? Quand ? Quelle est leur taille ? Quel appel téléphonique correspond à quel e-mail ? Les services secrets utilisent ces méthodes depuis longtemps. Il existe des programmes qui avertissent automatiquement quand quelqu'un suspect (comme le lecteur de *Hakin9*) change ses coutumes. Si cela vous intéresse, vous trouverez les informations plus détaillées sur l'analyse de trafic dans [5] ou – mieux encore – sur le projet TIA, futuristique et suspect, dans [8] et [9].

Les téléphones mobiles fournissent une information supplémentaire – ils permettent de vous localiser. La façon la plus primitive consiste à localiser la cellule (appartenant à une station de base) dans laquelle votre téléphone se trouve. Mais vous pouvez dire que la précision qui oscille entre 100 m et 10 km

ne vous intéresse pas. Vous vous trompez ! Imaginez que vous êtes dans un train de longue distance ou sur la gare. Ce voyage peut être facilement reconstitué à partir de la séquence radio cellule/temps. On peut déterminer sans problème quel train vous avez pris, à quelle vitesse vous vous êtes déplacés et quelle distance vous avez faite. Et tout cela peut être fait de façon automatique et sauvegardé pour plusieurs années, même si vous avez complètement oublié cet événement. Beaucoup de données inoffensives peuvent être transformées en données nocives. Lisez [5, 8.2] pour en savoir plus.

Est-ce une paranoïa ? Non, c'est de la pratique. On disait que la société Swisscom avait localisé les téléphones mobiles d'environ d'un million d'habitants pendant six mois, dans chaque minute (!), et ces données sont accessibles pour la police [12]. Aux États-Unis, les règlements concernant les services basés sur la localisation ont été déterminés par FCC [11]. Suivant ces règlements, depuis 2001, chaque téléphone mobile doit être localisé à l'intérieur de la zone de 125m pour 2/3 de temps (maintenant c'est plus précis). Et pourquoi ? Pour vous indiquer un magasin intéressant de l'autre côté de la rue, pour satisfaire à vos préférences personnelles. Nous en croyons. Mais sérieusement, ce n'est pas seulement une simple surveillance. En GB, le service de localisation au moyen des téléphones mobiles peut être utilisé pour localiser les enfants ; en Allemagne, le service similaire est préparé et discuté [6]. Et encore, les services basés sur la localisation peuvent aider à ranimer les consommateurs.

Les téléphones mobiles peuvent être localisés avec plus de précision que par cellule. Si vous vous déplacez d'une cellule vers une autre, votre téléphone doit passer aisément dans une nouvelle cellule. Cela exige qu'on doit savoir quand vous vous approchez du bord de la cellule. À son extrémité, la différence de la durée d'exécution entre les signals provenant des stations de base différentes est mesurée avec une grande précision pour chaque téléphone, et celui-ci envoie le résultat à la station de base actuelle (Figure 4). C'est une possibilité très importante. Si une cellule est trop sollicitée, une partie présélectionnée des téléphones peut être transférée vers les cellules voisines. Comme j'ai déjà mentionné – le système est constamment optimisé ! Les erreurs sont dues à la réflexion du signal (comme sur les façades) et limitées grâce au contact de plusieurs stations de base dans une ville.

Certes, il existe des données stockées concernant vos déplacements. Une question se pose : qui aura accès à ces données, et si ces données sont vraiment supprimées après un certain temps (comme cela est prévue par la loi) – et qui contrôlera tout cela ? Personnellement, je crois que dans la plupart des pays européens, les organes de polices ont un accès illimité aux données de localisation. Mais n'oubliez pas ce qui a été changé au nom de 2001.09.11. En GB, la protection des données privées est minimale, aux États-Unis, les données appartiennent à celui qui les a collectées (et il peut les vendre à volonté).

Une toute nouvelle astuce s'appelle *silent SMS*. La fonction nommée *stealth ping* est utilisée pour envoyer un SMS pour savoir si le téléphone est allumé et prêt pour roaming. Ce SMS n'est pas enregistré comme message dans votre téléphone, vous ne pouvez pas le voir. Mais il génère les données de connexion qui sont immédiatement récupérées par la police auprès de votre fournisseur. Comme ça, vous êtes localisés. Il est interdit aux detectives de suivre vos téléphones tout le temps, excepté les cas de graves délits. Mais ils peuvent vous envoyer un SMS silencieux et demander les données de connexion. Encore une fois, en Allemagne, a eu lieu une lutte contre ces méthodes.

Du point de vue technique, beaucoup d'autres choses sont possibles. La navigation GPS utilise les stations de base distantes

Références

[1] *http://www.isaac.cs.berkeley.edu/isaac/gsm.html*
[2] *http://www.ccc.de/gsm*
[3] *http://cryptome.org/a5.ps*
[4] *http://cryptome.org/gsm-crack-bbk.pdf*
[5] R.Wobst, *Abenteuer Kryptologie*, 3.Auflage, Addison-Wesley 2001
[6] *http://www.childlocate.co.uk*, *http://www.trackyourkid.de*
[7] R.Wobst, *Datenschutz: Komplexer, als es scheinen mag*, LanLine 4/2003, S.70-75 (AWi Verlag München) sur le Web (en allemande seulement) : *http://www.lanline.de/O/148/Y/82692/VI/10042982/VS/Datenschutz/default.aspx*
[8] *http://www.darpa.mil/iao/index.htm*
[9] *http://online.securityfocus.com/columnists/126*
[10] *http://www.research.att.com/~janos/3gpp.html*
[11] *http://www.fcc.gov/e911/enhanced*
[12] *http://www.fitug.de/debate/9712/msg00042.html*, *http://www.sonntagszeitung.ch/sz52/93419.HTM*
[13] B.Schneier, *Applied Cryptography*, 2nd ed., Wiley 1996

de centaines de kilomètres qui se mouvent à une vitesse de 8 km/s. Pourtant, cela permet de déterminer votre position dans la zone de quelques mètres. Les systèmes de navigation stationnaire l'utilisent pour localiser les bateaux et les avions depuis des dizaines d'années. Alors, deux de trois stations de base GSM peuvent, théoriquement, fixer le coin de votre bureau sur lequel se trouve votre téléphone – à moins que votre téléphone soit équipé pour ce type de tâche. Il faut prendre en considération la possibilité que ce type d'équipement peut devenir très populaire dans les années prochaines et du point de vue pratique rien ne changera.

Il est donc évident que votre fournisseur peut vous localiser, mais un detective amateur n'en est pas encore capable. Il doit être clair que vous n'avez que deux choix : utiliser le téléphone et devenir localisable ou l'éteindre complètement. Pourtant, la localisation n'est pas si dramatique que ça. Il faut seulement que vous vous en rendez compte. N'oubliez pas – cette possibilité peut s'avérer très utile dans un cas urgent.

Le futur : UMTS et A5/3

Probablement, GSM était la première application de masse utilisant les techniques cryptographiques. Pour cette tâche, le projet n'était pas si mauvais. Mais les concepteurs l'ont appris à partir des erreurs. La génération suivante des téléphones mobiles, connue en tant qu'UMTS, corrige les failles dans le projet GSM (cf. [5] et [10]).

- L'algorithme utilisé, KASUMI, a été révisé par plusieurs experts, il a été publié, il a résisté jusqu'alors à la cryptoanalyse, et il a la clé de 128 bits à la place de 64 bits. Les attaques comme sur A5/2 paraissent impossibles.
- De même, la station de base doit s'identifier auprès de votre téléphone. L'utilisation des dispositifs comme IMSI-catchers n'est plus possible.
- Les paquets de données possèdent les sommes de contrôle cryptographiques et comme ça, elles ne sont pas vulnérables aux attaques sur son chemin vers la station de base.
- Aussi les attaques répétées, p. ex. renvoi des paquets déjà envoyés à la station de base, peuvent être évitées car les paquets contiennent maintenant le numéro de séquence sécurisé.
- Le déchiffrement ne se fait pas toujours dans la station de base mais dans ce qu'on appelle *radio network controllers* (RNC). Cela permet de se connecter aux stations de base via la radio avec moins de risque.
- Une réauthentification rapide et sûre est possible, si la station de base ne doit pas envoyer des requêtes à l'ordinateur central. Cela permet les interruptions correctes de la connexion.

Du point de vue de la sécurité, la technologie UMTS constitue un grand progrès. L'unique problème est qu'elle n'est pas utilisée. D'une part, c'est à cause des problèmes financiers bien connus, et de l'autre part, il manque d'applications phares et de dispositifs appropriés. On dit que KASUMI sera aussi appliqué à GSM en tant que A5/3. L'échange des téléphones sera alors nécessaires dans quelques années.

Bien sûr, même un téléphone UMTS ne vous protège pas ni contre la localisation ni contre l'écoute de la part des autorités.

Conclusion

Les personnes qui peuvent écouter vos appels téléphoniques GSM n'utilisent pas de dispositifs achetés dans un supermarché, et de plus, il doivent être hautement qualifiés pour ce faire. C'est une technique d'espionnage très chère qui est probablement utilisée seulement par la police et certains services secrets – et, éventuellement, par la mafia car ce sont eux qui achètent de meilleurs spécialistes et dispositifs de services secrets mondiaux, comme cela montre l'exemple des trafiquants de drogue colombiens [7]. Une large surveillance au moyen de ces méthodes paraît impossible et ineffective. Mais l'espionnage industriel est bien possible.

C'est la localisation qui est plus dangereuse pour votre sécurité,. Mais n'oubliez pas que le scannage automatique des plaques d'immatriculation (comme un anneau d'acier en GB et Toll Collect system en Allemagne) est maintenant très populaire. De même, les cartes-client dans les supermarchés permettent d'extraire les données détaillés concernant le client, ainsi que chaque e-mail et chaque activité sur Internet génèrent les données qui peuvent ensuite être collectées et traitées.

Mais je crois que les avantages de la téléphonie GSM sont plus nombreux que les failles de sécurité. ■