État des lieux de la sécurité des communications cellulaires

Chaouki Kasmi et Benjamin Morin

ANSSI 51 bd. de la Tour Maubourg 75700 Paris Cedex 07 France

Résumé Le GSM fête cette année ses 20 ans d'existence. Le nombre d'utilisateurs est estimé à 80% de la population mondiale, soit 5 milliards d'individus dans plus de 200 pays [22]. La prolifération des terminaux mobiles et la multiplication de leurs usages (y compris dans des secteurs où ils sont utilisés pour des communications entre machines) imposent la satisfaction d'exigences de sécurité fortes.

Le thème de la sécurité des communications mobiles est vaste car il englobe celui de l'accès radio, de l'infrastructure des réseaux, des terminaux et des applications qui s'y exécutent. Cet article se focalise sur les deux premiers thèmes.

Depuis 2002, différents projets indépendants s'intéressent aux principes de sécurité mis en œuvre dans les réseaux de téléphonie mobile de 2ème et 3ème génération. Cette présentation dresse un panorama des objectifs et des impacts de ces projets sur la sécurité des réseaux de téléphonie mobile. Les principes de sécurité sont évoqués, ainsi que les problèmes de géolocalisation.

1 Introduction

Le thème de la sécurité des communications mobiles est vaste car il englobe celui de l'accès radio, de l'infrastructure des réseaux, des terminaux et des applications qui s'y exécutent.

De nombreux articles ont été publiés ces dernières années sur le thème de la sécurité des *smartphones*, en se focalisant essentiellement sur le domaine applicatif. Certains travaux récents portant sur les télécommunications cellulaires ont néanmoins fait des avancées significatives et ont démontré le réalisme d'attaques jusqu'alors réputées théoriques. Ces travaux pointent du doigt une certaine inertie dans la prise en compte des menaces, inertie qui tranche avec les mutations du secteur des terminaux dits intelligents. Cet article s'intéresse essentiellement à ces derniers travaux et présente un état des lieux de la sécurité des communications cellulaires et des projets indépendants qui s'y rapportent.

La première section situe le sujet de cet article dans le paysage actuel des télécommunications mobiles. L'article se poursuit par une description succincte des éléments qui composent un réseau de téléphonie mobile. Ces éléments sont nécessaires à la compréhension de la section 4, consacrée aux principes sur lesquels repose la sécurité des réseaux mobiles et à leurs vulnérabilités, et de la section 5, consacrée aux projets indépendants visant à analyser la sécurité de ces réseaux.

La section 6 aborde les problèmes de géolocalisation et la dernière conclue l'article.

2 Contexte technique et économique

Le secteur de la téléphonie mobile a connu de profondes mutations en l'espace de quelques années. Le phénomène dit de « convergence » a progressivement transformé des téléphones portables simples (« *feature phones* ») en terminaux multi-fonctions beaucoup plus sophistiqués (« *smart phones* »).

Pour accompagner cette transformation, ce secteur initialement réservé à un nombre limité d'acteurs (fabricants de terminaux et opérateurs de réseaux de télécommunications [1]) s'est ouvert à d'autres, tels que les développeurs de systèmes d'exploitation ou d'applications, les fournisseurs de contenus, les utilisateurs professionnels, etc. Avec un support adéquat du matériel, les systèmes d'exploitation doivent apporter des garanties d'intégrité et d'isolation afin par exemple d'empêcher une application malveillante de perturber le réseau de télécommunication (que cette application soit installée de façon délibérée ou non par le porteur du terminal). Les utilisateurs n'ont alors pas la possibilité de contrôler intégralement leur terminal. Ce dernier point est un exemple de différence notable entre le modèle de sécurité des terminaux mobiles et celui des ordinateurs, qui illustre la difficulté à concilier les exigences de sécurité des différents acteurs de la téléphonie mobile.

Le besoin de séparer les domaines d'exécution des différentes parties se traduit au niveau de l'architecture logique et physique des plateformes mobiles. Comme nous le verrons dans la section suivante, les plateformes matérielles distinguent généralement le domaine applicatif, au sein duquel sont exécutées les applications de l'utilisateur, du domaine radio, qui gère les communications avec le réseau.

Comme évoqué précédemment, le secteur de la téléphonie mobile est resté clos pendant longtemps. Son ouverture relativement récente est a priori positive sur le plan de la sécurité car elle concourt à une meilleure confiance dans les terminaux, en permettant aux utilisateurs de mieux maîtriser leur fonctionnement. Cette ouverture demeure cependant partielle, et ce pour plusieurs raisons. Elle l'est parce que certains acteurs majeurs (Apple et RIM en particulier) maîtrisent intégralement la chaine de conception des terminaux, depuis la plateforme matérielle jusqu'à la distribution des applications. Le rachat récent de Motorola par Google semble d'ailleurs indiquer que cette « verticalisation » du marché s'accentue. L'ouverture est aussi et surtout partielle parce qu'elle se limite au domaine applicatif des terminaux ; le domaine radio demeure quant à lui relativement opaque.

1. Les fabricants de cartes à puce sont aussi des acteurs du secteur via les cartes SIM, mais ils n'interviennent pas directement sur la conception des terminaux et les éléments du réseau de télécommunication.

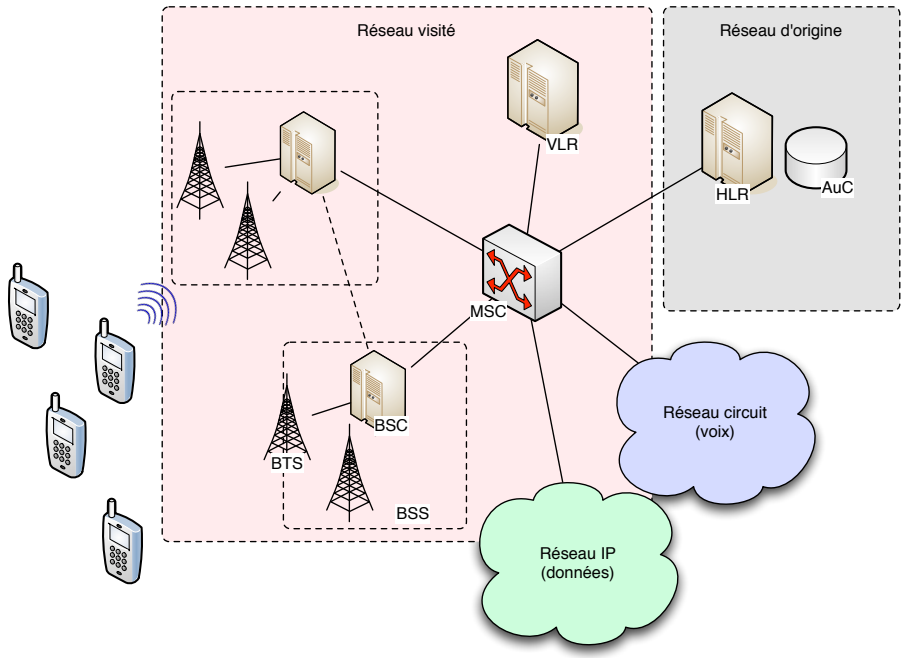

Figure 1. Architecture type d'un réseau cellulaire GSM

3 Éléments d'architecture

Cette section propose un survol des principaux éléments qui composent un réseau cellulaire. Nous séparons cette description en deux parties : la première est consacrée à l'infrastructure du réseau cellulaire et la seconde à l'architecture des terminaux mobiles (également appelés stations mobiles, ou *mobile equipement*, ME).

3.1 Architecture d'un réseau cellulaire

Les éléments qui composent un réseau cellulaire et la façon de les désigner ont évolué avec les différentes générations de systèmes de télécommunications (GSM, EDGE, UMTS, etc.). La description qui suit est délibérément simple. Nous ne rentrons pas dans les détails afin de faciliter la compréhension des sections suivantes. Nous renvoyons le lecteur intéressé aux ouvrages spécialisés sur ce sujet [24].

Comme l'illustre la figure 1, une infrastructure de télécommunication cellulaire distingue deux types réseaux : le réseau d'*origine*, c'est-à-dire le réseau de l'opérateur avec lequel l'usager souscrit un abonnement, et le réseau *visité*, qui

peut appartenir à un opérateur différent du précédent. Le réseau visité achemine les communications voix et/ou données de l'usager une fois que le terminal de ce dernier s'est correctement authentifié auprès de son réseau d'origine.

On peut distinguer deux principaux sous-systèmes :

- Le sous-système radio (*Base Station Subsystem, BSS*) assure les transmissions radio-électriques et gère les ressources radio. Il est constitué de stations de base (*Base Transciever Station*, BTS [2]) qui communiquent avec les stations mobiles par un lien radiofréquence, communément appelé « interface air ». Des équipements appelés *Base Station Controler* (BSC) contrôlent les stations de base ;
- Le sous-système réseau comprend des fonctions nécessaires à l'établissement des appels et à la mobilité. Il est notamment constitué de bases de données et de commutateurs :
  - Le centre de commutation des services mobiles (*Mobile Switching Center*, MSC) relie des contrôleurs de station de base au réseau téléphonique public (liaison voix) et à Internet (liaison de données) ;
  - Le HLR (*Home Location Register*) est une base de données de localisation et de caractérisation des abonnés. Pour les besoins d'itinérance, certaines données sont transmises à la base de données de la cellule visitée (*Visitor Location Register*, VLR).

Un élément important de l'architecture est le centre d'authentification (*Authentication Center*, AuC), qui dispose des éléments nécessaires à la sécurisation des communications, notamment les clés cryptographiques associées aux usagers. Ces clés servent notamment à dériver des clés temporaires qui sont transmises par l'AuC au MSC. La section 4 précise les échanges correspondants.

3.2 Architecture des terminaux

L'architecture logique type des smartphones actuels distingue généralement deux environnements d'exécution distincts. Le premier correspond au système d'exploitation applicatif, qui assure notamment l'exécution des applications de l'utilisateur. Le second correspond à la pile logicielle responsable des communications réseau (GSM, 3G, etc.). Ce dernier environnement est généralement appelé le *baseband*. Cette architecture logique peut se décliner sous différentes architectures physiques. Certains terminaux utilisent deux processeurs distincts, physiquement séparés et reliés par un bus de communication. Ces deux processeurs peuvent également être inclus dans une même puce (*system-on-chip, SOC*). D'autres solutions consistent à utiliser des machines virtuelles pour réaliser la séparation des deux environnements d'exécution sur un seul et même processeur.

Dans tous les cas, les principes de conception des environnements d'exécution des *basebands* ont peu évolué depuis les débuts de la téléphonie mobile : ils sont généralement exempts des protections standards disponibles sur les processeurs de plus haute gamme (unité de gestion de la mémoire ou *MMU*, par exemple) et

2. On trouve aussi l'appellation BST, *Base Station Trancievер.*

leur code obéit souvent aux pratiques de développement en vigueur au début des années 90, pratiques qui ne mettaient pas nécessairement l'accent sur la sécurité. La présence de failles logicielles au sein de ces environnements d'exécution est donc à craindre, et leur exploitation pourrait avoir des conséquences importantes en l'absence de mécanisme d'isolation entre les tâches.

La carte SIM (*Subscriber Identity Module*) [12,11] peut également être considérée comme un environnement d'exécution distinct, même si celui-ci est beaucoup plus restreint que les deux précédents. La carte SIM est en effet une carte à puce qui dispose d'une capacité de calcul et qui renferme notamment les éléments d'identification du terminal et de son porteur ainsi que des clés cryptographiques. Son rôle est fondamental dans la sécurisation des télécommunications mobiles. Cette carte appartient à l'opérateur car c'est par elle que passent les autorisations d'accès au réseau. Les cartes USIM (*Universal SIM*) [10,13] sont fonctionnellement équivalentes aux cartes SIM ; elles renferment les mécanismes cryptographiques utilisés dans le cadre des réseaux de téléphonie mobile de troisième génération. Dans l'avenir, l'élément de confiance que représente la carte USIM aura vocation à héberger des applications tierce partie pour des usages de type NFC (*Near-Field Communication*), tels que le paiement sans contact ou le contrôle d'accès. La validation des applications incluses au sein des cartes USIM sera alors primordiale, afin d'empêcher un attaquant d'implanter une application malveillante au sein de cet élément de confiance.

4 Mécanismes de sécurité des réseaux de mobiles

Cette section propose un survol des nombreuses familles de cryptosystèmes utilisés dans les réseaux de télécommunication mobiles pour satisfaire les exigences de confidentialité et d'intégrité des communications et pour authentifier les terminaux mobiles. L'emploi de tel ou tel cryptosystème dépend de la fonction de sécurité visée (authentification, négociation de clé, chiffrement, intégrité), de l'opérateur du réseau de télécommunication et de la génération de réseau considérée. Nous séparerons cette dernière en deux catégories principales : les réseaux GSM (2G), GPRS (2.5G) et EDGE (2.75G), d'une part, et les réseaux UMTS (3G) et LTE (4G), d'autre part (voir figure 5).

Nous débutons cette section par une présentation des éléments utilisés pour identifier les terminaux mobiles. Nous la concluons par un commentaire sur une exigence de sécurité souvent négligée et pourtant essentielle dans le cas des réseaux de télécommunication : la disponibilité.

4.1 Eléments d'identification

On distingue deux principaux éléments d'identification dans les terminaux mobiles selon qu'ils concernent le terminal ou son porteur. Ils sont utilisés dans toutes les générations de réseau (2G à 4G).

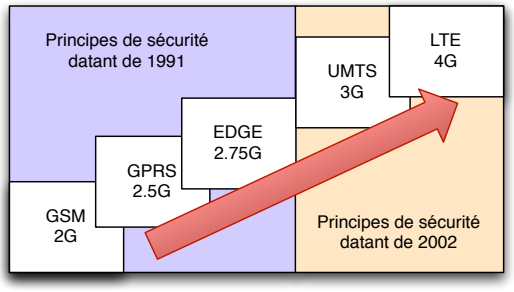

Figure 2. Evolution des réseaux de téléphonie mobile

L'IMSI (*International Mobile Subscriber Identity*) est un numéro unique permettant à l'opérateur du réseau d'identifier le *porteur* du terminal mobile. Il est stocké dans la carte SIM et est constitué des indicatifs du pays d'origine du porteur (le MCC, *Mobile Country Code*, qui vaut par exemple 208 pour la France) et de l'opérateur (le MNC, *Mobile Network Code*), ainsi que du numéro de l'abonné.

L'IMSI est envoyé en clair aux antennes relai lors du protocole initial d'authentification du terminal auprès du réseau. Afin d'empêcher un attaquant d'identifier et de traçer le porteur d'un terminal à l'aide d'un dispositif d'écoute de communication radio, un numéro temporaire appelé TMSI (*Temporary IMSI*) est attribué au porteur par l'opérateur. Le TMSI est utilisé en lieu et place de l'IMSI dans la suite des communications et seul l'opérateur est en mesure d'établir la correspondance entre l'IMSI et le TMSI.

L'IMEI (*International Mobile Equipement Identity*) est un numéro supposé unique permettant à l'opérateur d'identifier le terminal mobile. Il est constitué des numéros de série et de modèle [3] de l'équipement, ainsi que d'un code de contrôle (formule de Luhn). L'IMEI sert notamment à empêcher un terminal volé ou perdu de joindre le réseau de communication.

En ce qui concerne le réseau, des informations d'identification sont diffusées par l'opérateur au travers des antennes relais et à destination des terminaux mobiles. On y retrouve par exemple le MCC, le MNC, et les informations permettant aux stations mobiles de se connecter au réseau d'opérateur.

4.2 Authentification des équipements mobiles

Hormis le besoin évident de facturation des communications, l'authentification forte des terminaux mobiles vise à contrer des tentatives d'usurpation

3. L'identifiant de modèle, appelé TAC (*Type Allocation Code*), est propre à un fabricant de terminal et est délivré par une autorité de certification centrale.

d'identité d'un abonné. A noter que l'authentification dont il est question ici est bien celle du terminal vis-à-vis du réseau ; le porteur s'authentifie pour sa part auprès de son terminal (plus exactement, sa carte SIM) par la saisie de son code PIN.

Le mode d'authentification des terminaux mobiles est probablement l'évolution la plus importante entre les deux grandes familles de réseaux. Dans le cas des réseaux 2G, l'authentification est unilatérale : seul le terminal s'authentifie auprès du réseau d'opérateur. Dans le cas des réseaux 3G, l'authentification est mutuelle. Cette évolution est fondamentale car elle permet de contrer des attaques par le milieu, dans lesquelles un adversaire tente de se faire passer pour le réseau de l'opérateur auprès du terminal d'un abonné et tenter ensuite d'intercepter ses communications.

Le protocole d'authentification utilisé dans les réseaux GSM repose sur un cryptosystème symétrique appelé A3. L'authentification unilatérale du terminal consiste pour ce dernier à calculer un code d'authentification de message (MAC) en réponse à un challenge RAND envoyé par l'opérateur. Ce challenge est un aléa généré par le *centre d'authentification* (AuC) de l'opérateur, puis acheminé jusqu'au terminal via un centre de commutation (MSC), puis une station de base.

Le calcul de la réponse au challenge, désigné SRES, nécessite une clé symétrique partagée, K_i, connue exclusivement de la carte à puce et de l'AuC [4]. Le calcul de SRES est réalisé conjointement par la carte à puce et par l'AuC. Ce dernier communique SRES au MSC, qui peut ainsi le comparer au SRES envoyé par le terminal en réponse au challenge. L'authentification est acceptée en cas d'égalité. Ce protocole est résumé en figure 3.

Un algorithme de dérivation de clé appelé A8 est utilisé pour produire une clé symétrique K_c à partir de K_i et de RAND. Cette clé de session K_c sert à chiffrer les communications ; elle est générée par la carte à puce du terminal, d'une part, et par l'AuC d'autre part. La carte à puce fournit K_c au terminal, tandis que l'AuC la fournit au MSC, qui la transmet à l'antenne relais. Le chiffrement des communications est donc ensuite réalisé entre le terminal et l'antenne relais.

On peut noter que les algorithmes A3 et A8 ne sont pas normalisés, ce qui signifie que les opérateurs sont libres d'utiliser des algorithmes propriétaires non publics. Ces algorithmes doivent en principe avoir de bonnes propriétés cryptographiques afin de résister à des attaques, mais ce n'a pas toujours été le cas. Ainsi, l'algorithme COMP128 a par exemple été utilisé alors qu'il était vulnérable et permettait au détenteur d'une carte SIM de cloner celle-ci avec quelques dizaines de milliers de couples RAND/SRES.

Le protocole d'authentification utilisé dans les réseaux de troisième génération permet au terminal et au réseau de l'opérateur de s'authentifier

4. L'AuC dispose de la base de données des correspondances entre les IMSI et les clés K_i des abonnés.

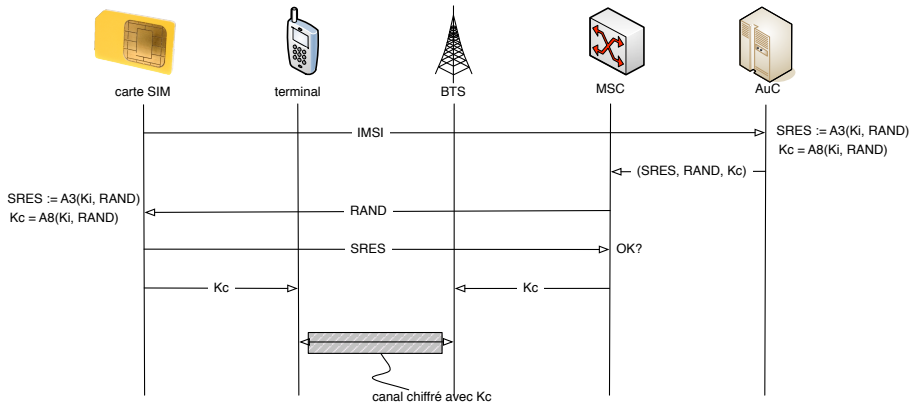

Figure 3. Principe d'authentification dans le cadre de réseau de 2ème génération (GSM)

mutuellement. La protection des communications dans les réseaux de troisième génération repose sur un ensemble de fonctions de dérivation de clés et une clé symétrique maîtresse K, qui joue un rôle analogue à la clé K_i des réseaux de seconde génération. La clé K est notamment impliquée dans le calcul (non détaillé ici) d'un jeton d'authentification AUTN, qui est envoyé par l'AuC au terminal mobile en plus de l'aléa RAND. Ce jeton permet à la carte USIM du terminal d'authentifier le réseau de l'opérateur avant d'envoyer à son tour la réponse au challenge.

Milenage [9] est un algorithme fondé sur AES qui est par exemple utilisé pour l'authentification et la dérivation de clés dans les réseaux UMTS.

A l'instar de la fonction A8 du GSM, une fonction de dérivation produit une clé CK (analogue à la clé K_c) utilisée pour chiffrer le trafic de données et de signalisation. Une autre fonction de dérivation génère également une clé IK (*Integrity Key*) utilisée pour l'intégrité des échanges.

La figure 4 illustre le déroulement du protocole d'authentification de la 3G.

4.3 Confidentialité et intégrité des communications

Des algorithmes cryptographiques sont mis en œuvre dans le but de protéger la confidentialité des données échangées. Ces algorithmes plus ou moins robustes en fonction du protocole mis en œuvre ont pour but de protéger les communications radiofréquences. Notons que la protection en confidentialité est optionnelle (le chiffrement est à l'initiative du réseau).

La confidentialité dans les réseaux de seconde génération repose sur l'emploi de la clé K_c et d'un algorithme de chiffrement à flot normalisé désigné

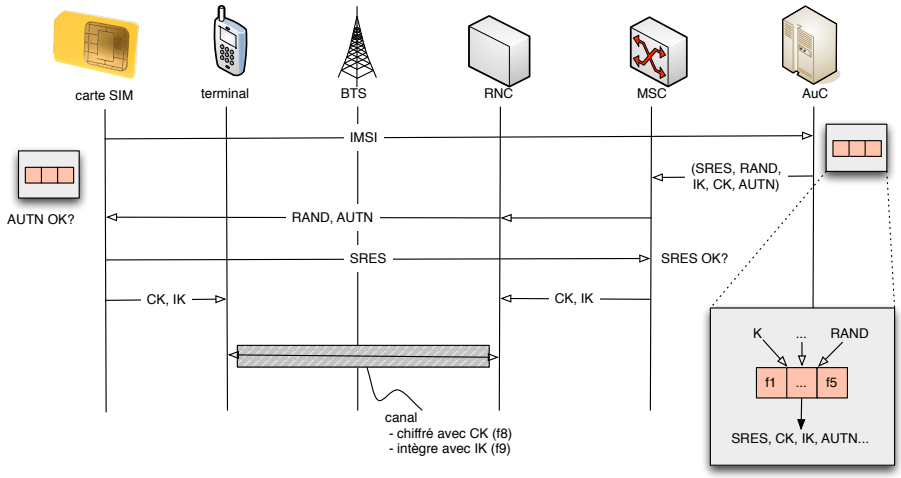

Figure 4. Authentification mutuelle en 3G

A5. Le chiffrement porte sur l'ensemble du trafic et de la signalisation. Il existe en fait quatre algorithmes de chiffrement désignés A5/1 à A5/4. Le choix de l'algorithme à utiliser pour une communication fait l'objet d'une négociation, le réseau choisissant un algorithme dans la liste de ceux que lui propose le terminal. Cette liste contient au moins A5/1. Dans le cas du GPRS, les algorithmes GEA sont utilisés [7,8].

L'algorithme A5/1 est massivement déployé, mais n'offre pas une protection absolue en confidentialité. Plusieurs attaques « à clair connu » contre A5/1 ont en effet été publiées depuis la fin des années 1990 [15,17,14]. Ces attaques permettent à un adversaire passif [5] disposant de tables précalculées et de la connaissance d'une partie du trafic clair de déchiffrer une communication en quasi-temps réel. La quantité de données claires nécessaire (issues du trafic de signalisation et/ou de *padding* constant) et surtout le volume des tables précalculées constituaient les principaux obstacles à la réalisation pratique des attaques. En 2010, Karsten Nohl a finalement fait une démonstration publique de déchiffrement de communications chiffrées avec A5/1 à l'occasion du Chaos Computer Congress [27].

L'algorithme A5/2 a essentiellement été conçu pour l'export et n'est utilisé que dans un nombre restreint de pays où la législation en matière de chiffrement est restrictive. Des attaques très réalistes ont été publiées contre A5/2.

Les algorithmes A5/3 [7] et A5/4 [8] sont dérivés de l'algorithme Kasumi utilisé dans la 3G. Ces algorithmes ont été spécifiés plus tardivement (2002) et leur déploiement demeure limité. En 2010, des faiblesses ont été identifiées dans l'algorithme Kasumi [16], mais elles ne permettent toutefois pas de réaliser des

5. C'est-à-dire disposant d'un équipement d'écoute des communications radio.

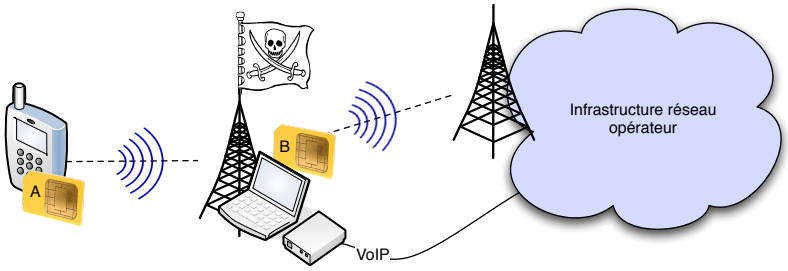

Figure 5. Attaque *man in the middle* dans un réseau cellulaire

attaques pratiques à l'heure actuelle.

L'absence d'attaque pratique contre les algorithmes A5/3 et A5/4 n'élimine pas pour autant la menace d'une interception des communications par un attaquant *actif*. Compte tenu de l'absence d'authentification du réseau par le mobile et du fait que c'est *in fine* le réseau qui choisit l'algorithme de chiffrement, un attaquant disposant d'une fausse station de base peut en effet déchiffrer les communications des terminaux qui s'y connectent.

Une façon de procéder consiste pour l'adversaire à forcer l'utilisation d'un canal de communication en clair, ou bien d'un algorithme faible (par exemple A5/2) pour reconstituer la clé K_c. En théorie, l'utilisation d'un canal de communication non chiffré doit être indiqué sur les terminaux, mais ce n'est pas toujours le cas en pratique.

Notons par ailleurs qu'un terminal peut réutiliser la même clé K_c et le même aléa entre des communications chiffrées en A5/1 et A5/3. Après avoir enregistré une communication chiffrée en A5/3 entre un terminal et une station de base légitime, un attaquant muni d'une fausse station de base peut ainsi négocier la réutilisation de la clé de chiffrement K_c dans le cadre d'une communication en A5/1 avec le terminal. L'attaquant peut ensuite obtenir K_c en appliquant les attaques mentionnées ci-dessus sur du trafic de service (*idle frames*) et ainsi déchiffrer le trafic initialement enregistré.

La section 5 donne plus de détails sur les projets de développement d'outils d'analyse GSM.

La confidentialité dans les réseaux de troisième génération repose sur l'utilisation de deux nouveaux algorithmes de chiffrement, Kasumi et Snow 3G, et de clés de plus grande taille (128 bits). Ces deux algorithmes sont également utilisés pour assurer l'intégrité des communications.

Kasumi est un algorithme de chiffrement par blocs utilisé par défaut dans les réseaux UMTS. Snow 3G est un algorithme de chiffrement à flot « de repli »,

dans l'hypothèse où KASUMI serait cassé. Cet algorithme est implanté au sein des terminaux mobiles actuels, mais pas nécessairement dans les équipements d'infrastructure des opérateurs. Comme évoqué précédemment, une attaque « à clés reliées » contre KASUMI a été publiée en 2010 [16], mais le modèle d'attaque considéré est peu réaliste et ne remet pas en cause la sécurité pratique du GSM et de l'UMTS.

Les réseaux de troisième génération apportent donc des améliorations significatives en matière de confidentialité. Le chiffrement demeure à l'initiative du réseau (qui peut décider de rester en clair), cependant le réseau doit authentifier l'ordre de rester en clair, donc être reconnu de l'opérateur d'origine. Les attaques par fausses stations de base sont donc inopérantes.

Les algorithmes de chiffrement et d'intégrité ont été partiellement renouvellés dans le cas des réseaux de quatrième génération. Ils s'appuient sur deux algorithmes, respectivement fondés sur SNOW 3G et AES. Des discussions sont en cours pour intégrer un troisième jeu d'algorithmes, baptisé ZUC [20], à la demande de la Chine, mais plusieurs failles majeures ont été identifiées dans les spécifications intermédiaires de cet algorithme [21].

Notons enfin que les réseaux de troisième génération incluent un équipement appelé RNC (c.f. figure 4) jusqu'auquel se prolonge le chiffrement des communications (celui-ci se termine au niveau des BTS dans le cas du GSM). La protection physique de cet équipement est meilleure que celle des BTS.

4.4 Disponibilité

Le terme « disponibilité » peut soit s'interpréter comme la capacité du réseau de l'opérateur à résister à des attaques visant à le rendre inopérant (c.-à-d. sa résilience), soit être associé à la couverture radiofréquence sur un territoire donné pour les différents services voix et données des réseaux GSM, GPRS, EDGE et UMTS. Nous abordons ici ces deux interprétations.

Disponibilité/couverture : cette interprétation de la disponibilité peut a priori sembler étrangère aux problèmes de sécurité, mais elle a pourtant une importance. Malgré les investissements réalisés par les opérateurs [30], la couverture réseau du territoire en 3G demeure inférieure à celle du GSM et varie selon les opérateurs [28,29,32]. Tous les usagers ne disposent donc pas d'alternative plus sécurisée au GSM, ce qui empêche de « bloquer » les terminaux en 3G. Les problèmes évoqués précédemment demeurent donc d'actualité. En France, la technologie 4G en est encore au stade expérimental (d'autres pays comme les États-Unis ont fait le choix de passer directement à la 4G).

Disponibilité/résilience : la disponibilité revêt une importance toute particulière dans le cas des réseaux cellulaires car les terminaux mobiles se substituent de plus en plus aux terminaux fixes.

La disponibilité au sein des réseaux GSM repose en partie sur l'hypothèse que les terminaux mobiles se comportent « correctement » vis-à-vis du réseau.

L'opacité des principes de conception des terminaux mobiles, qui a prévalu pendant longtemps, a largement contribué à ce que cette hypothèse soit considérée valide car elle complexifie la recherche de vulnérabilités.

Cependant, des projets indépendants d'analyse des principes de conception des équipements utilisés dans un réseau GSM ont récemment mis en évidence des vulnérabilités sur certains équipements. Des failles d'implémentation logicielle sont susceptibles d'être déclenchées à distance par l'envoi de trames malformées et provoquer un blocage d'équipements d'infrastructure.

Un effet analogue peut également être obtenu par des attaques visant à épuiser les ressources des équipements par l'envoi de requêtes en rafale. Il a notamment été montré [31] que l'envoi massif de trames (correctes sur le plan protocolaire) peut provoquer une surconsommation de mémoire au niveau des BTS et engendrer un déni de service. Ces attaques ne sont pas facilement contrables sans un mécanisme de gestion de la mémoire robuste.

Il est donc nécessaire que les équipements soient soumis à des tests stricts afin que les déploiements actuels et futurs ne soient plus vulnérables à des attaques en disponibilité des réseaux d'opérateur.

5 Projets indépendants d'analyse des réseaux de télécommunication

Les attaques actives dans les réseaux GSM ou UMTS nécessitaient jusqu'à récemment des dispositifs qui étaient onhéreux et/ou difficiles à se procurer pour un individu, et dont les principes de conception ne sont pas publics. Les informations disponibles pour l'analyse de la robustesse des mécanismes de protection sont très théoriques et ne reflètent pas nécessairement les implémentations réelles.

La difficulté d'analyse des spécifications techniques a poussé la communauté de chercheurs en sécurité des systèmes d'information et de communication à réaliser une retro-conception des équipements de télécommunication. Ces projets portent sur des équipements mobiles et de cœur de réseau et permettent d'émuler un réseau d'opérateur complet.

5.1 Outils d'analyse passifs

Les équipements de radiocommunication ont connu une évolution très forte ces dernières années avec l'avènement de la radio logicielle (*Software Defined Radio, SDR*). Le domaine s'est ouvert à une nouvelle communauté de développeurs et n'est plus réservé aux spécialistes ; des équipements dédiés à la numérisation à la volée permettent aujourd'hui l'acquisition de signaux [6] et leur analyse à l'aide de bibliothèques de traitement numérique du signal telles que GNURadio [6]. Récemment, des terminaux mobiles d'ancienne génération [26] ont été reconfigurés afin d'exploiter l'architecture matérielle dédiée à l'application de téléphonie mobile (numérisation, décodage...).

6. Voir notamment `http://www.ettus.com/`

Le projet Airprobe [1] propose les éléments de conception d'un outil d'analyse passif des trames radiofréquences afin d'évaluer la sécurité en confidentialité du protocole GSM. Il est constitué des modules d'acquisition, de démodulation et d'analyse.

Les attaques visant à retrouver efficacement une clé de chiffrement GSM reposent sur un compromis temps/mémoire qui nécessite de précalculer des tables. Le projet « The Kraken » [5] a notamment eu pour objet la construction de telles tables, en ayant recours à des optimisations pour réduire l'espace nécessaire à leur stockage et le temps de calcul. De plus, des attaques fonctionnelles ont été dévoilées portant sur les algorithmes GEA utilisés en GPRS et EDGE [25].

5.2 Outils d'analyse actifs

Plusieurs projets complémentaires portent sur la conception des équipements qui participent au fonctionnement d'un réseau de téléphonie mobile. Ces projets ont été réalisés par rétro-conception d'équipements existants, par analyse protocolaire et par l'étude des spécifications techniques.

Le projet OsomcomBB [4,34] propose une implémentation logicielle ouverte d'un *baseband* et de sa pile protocolaire GSM. Cet outil sert à émuler un téléphone mobile. La maîtrise complète du déroulement du protocole GSM que confère cette implémentation ouverte permet notamment à un auditeur de sécurité d'évaluer la robustesse des implémentations de piles protocolaires fermées.

D'autres projets portent sur la réalisation d'équipements réseau sur une base de radio logicielle. Le projet OpenBTS [3] a ainsi pour objectif de concevoir une station de base GSM et GPRS. Il est complété par le projet OpenBSC [2], qui porte sur la conception d'un contrôleur de stations de base GPRS, EDGE et UMTS. Il est important de noter que l'attaque par fausse station de base est limitée aux appels émis depuis l'équipement mobile cible, comme le terminal n'est plus lié à son opérateur de téléphonie mobile le routage des données depuis le réseau légitime ne peut plus être réalisé.

La simulation d'un réseau d'opérateur avec des équipements maîtrisés permet également d'étudier la robustesse des *basebands*. Weinmann [33] a montré que les logiciels exécutés au sein des *basebands* ne sont pas exempts de bogues et qu'il est possible d'exécuter du code arbitraire sur les *basebands* en leur adressant des messages malformés. Il existe d'ailleurs des projets de conception de *fuzzers* basés sur OpenBTS, visant à automatiser la détection de vulnérabilités sur différents modèles de *basebands* [23]. L'absence de protections standards au sein de ces environnements d'exécution expose donc les terminaux mobiles à une prise de contrôle de la partie radio des terminaux par un attaquant. De telles attaques sont certes très spécifiques (leur succès depend entre autres du système d'exploitation et de l'architecture matérielle des équipements), mais il existe relativement peu de fabricants de basebands et les mêmes équipements sont souvent utilisés dans différents modèles de terminaux. La prise de contrôle d'un nombre important de *basebands* pourrait alors servir à provoquer un déni de service sur les infrastructures réseau des opérateurs [23]. L'extension de la prise

de contrôle du *baseband* à l'environnement d'exécution applicatif du terminal constitue également une menace crédible.

6 Gestion de la mobilité et géolocalisation

La protection en confidentialité et en intégrité des communications n'est qu'un élément parmi les exigences de sécurité que la téléphonie mobile doit satisfaire. La protection des données à caractère personnel est un autre problème. Cette section se penche plus particulièrement sur la protection des données de localisation géographique des usagers. Nous n'abordons pas ici les informations fournies par des puces GPS implantées au sein de certains terminaux, mais celles qui émanent des réseaux cellulaires.

La géolocalisation est inextricablement liée à la mobilité. L'opérateur a en effet besoin de connaître le positionnement géographique des terminaux à des fins de routage des communications (gestion de l'itinérance, ou *roaming*). Dans le cas des réseaux GSM, l'opérateur gère une base de donnée centrale, appelée HLR (*Home Local Register*), au sein de laquelle la position de chaque abonné est renseignée et mise à jour régulièrement. Cette information permet de connaître l'adresse réseau du MSC auquel le mobile est rattaché à un instant donné.

Plusieurs techniques de géolocalisation GSM existent. La plus répandue, appelée Cell ID, repose sur la connaissance du positionnement géographique des antennes relais GSM. Il est possible de calculer par triangulation la position d'un terminal à partir des antennes relais environnantes auxquelles celui-ci est connecté. La précision de la position dépend de la densité d'antennes à un emplacement donné et peut aller de quelques dizaines de mètres à plusieurs kilomètres [18]. Plusieurs projets privés ou communautaires de cartographie des réseaux GSM constituent des bases de données établissant le lien entre les identifiants de cellules et leur position géographique [7].

Des sociétés telles qu'Apple, Google ou Microsoft, qui disposent de terminaux largement déployés et équipés de puces GPS, peuvent « déléguer » cette cartographie à leurs utilisateurs [8]. Alternativement, les techniques dites de *War Driving* [25] recensent également les identifiants de cellules GSM et Wi-Fi environnantes. Le projet WASP [9] (*Wireless Aerial Surveillance Platform*) propose même d'utiliser des drones à cet effet. Parallèlement, des applications malveillantes ont également été diffusées afin de localiser des abonnés en temps réel en exploitant les périphériques radios Wi-Fi, GSM/UMTS et GPS.

La géolocalisation a plusieurs applications légitimes, qui répondent à un besoin des utilisateurs. D'autres applications sont litigieuses (par exemple, le marketting ciblé), voire illégales (espionnage). Hormis quelques applications très spécifiques pour lesquelles un encadrement strict est nécessaire (par exemple,

7. Voir par exemple `http://www.opencellid.org/`, `http://crowdflow.net/`.
8. Chaque terminal est en mesure d'enregistrer la localisation géographique des stations de base environnantes à l'aide des informations fournies par sa puce GPS.
9. `https://www.defcon.org/html/defcon-19/dc-19-speakers.html#Tassey`

la localisation de personnes en détresse), la divulgation et/ou l'utilisation des données permettant de positionner un individu devraient donc requérir le consentement explicite de ce dernier. Plusieurs affaires récentes ont montré que ce n'est pas toujours le cas (voir par exemple l'application iPhoneTracker [10]).

7 Conclusion et recommendations

Cet article s'est focalisé sur les mécanismes et les problèmes de sécurité associés à la couche radio des réseaux de télécommunication cellulaires, tant sur le plan protocolaire que sur celui des équipements terminaux qui les composent.

La migration progressive des protocoles de seconde génération vers ceux de troisième et quatrième génération apporte des améliorations significatives en matière de sécurité des échanges. L'authentification mutuelle d'un terminal et du réseau de l'opérateur et l'utilisation d'algorithmes de chiffrement robustes font partie de ces améliorations notables. Toutefois, la couverture des protocoles de dernière génération au niveau du territoire demeure inférieure à celles des protocoles plus anciens, tels que le GSM. Les faiblesses intrinsèques de ce dernier, qui mettent notamment en péril la confidentialité des échanges, sont connues sur le plan théorique depuis plus de dix ans et sont maintenant exploitables en pratique pour un coût modique. En attendant une généralisation des réseaux UMTS et LTE, ces vulnérabilités militent en faveur de l'utilisation de l'algorithme A5/3 au sein des réseaux GSM afin d'empêcher *a minima* les interceptions passives de communications.

La réalisation pratique de ces attaques a en partie été rendue possible par les travaux d'analyse et de rétro-conception de chercheurs indépendants. Ces travaux ont également pointé du doigt des vulnérabilités logicielles sur les équipements terminaux des réseaux cellulaires, à savoir les *basebands* (du côté des terminaux mobiles) et les stations de base (du côté de l'infrastructure des opérateurs). L'opacité des principes de conceptions de ces équipements complexifie les audits de sécurité visant à évaluer leur robustesse. Il est pourtant nécessaire d'entreprendre de telles évaluations, car la présence de vulnérabilités au sein ces équipements constitue une menace tout à fait crédible.

Plusieurs projets communautaires visant à concevoir les équipements d'un réseau cellulaire ont ainsi vu le jour ces deux dernières années. Ces travaux peuvent faciliter les évaluations de sécurité des équipements, évaluations qui seraient à même d'améliorer la confiance globale dans la robustesse des réseaux cellulaires.

Ces mêmes travaux permettent en contrepartie à des individus malveillants de mettre en place des dispositifs d'interception actifs et/ou d'identifier des vulnérabilités au sein des équipements terminaux. L'exploitation de ces vulnérabilités pourrait mettre en péril la confidentialité, l'intégrité et la disponibilité des réseaux cellulaires. C'est la raison pour laquelle il est nécessaire d'encadrer strictement les travaux d'analyse de ces réseaux. Notons à ce sujet que

10. `http://petewarden.github.com/iPhoneTracker/`

les équipements d'analyse dont il est question font partie des appareils dont l'utilisation est régie par les articles R226 du code pénal.

En particulier, l'atteinte à la disponibilité des réseaux de cellulaires pourrait avoir des répercussions graves. L'utilisation de ces réseaux n'est en effet plus « limitée » aux seules communications entre individus. Elle s'étend également aux communications « de machine à machine » et ce dans de nombreux secteurs, incluant ceux d'importance vitale (transports, énergie, etc.).

En ce qui concerne les problématiques de géolocalisation, il est nécessaire de laisser aux usagers le choix de divulguer ou non à des tiers les informations présentes sur leur terminal qui permettent de les localiser. Les opérateurs doivent pour leur part limiter la fourniture des données de localisation nécessaires au routage à des applications extrêmement spécifiques et encadrées par la loi. La CNIL s'est par ailleurs prononcée à plusieurs reprises sur ce sujet [19].

La question du contrôle des informations de localisation par les usagers pose celle, plus générale, de la maîtrise des terminaux par leurs utilisateurs (particuliers ou institutionnels). De ce point de vue, le modèle de sécurité des *smartphones* est différent de celle des ordinateurs conventionnels car les terminaux n'« appartiennent » pas complètement à leurs usagers. Ceci s'explique en partie par le nombre de parties prenantes au niveau de chaque terminal mobile, parties dont les exigences ne sont pas nécessairement les mêmes que celles des usagers. La confiance globale dans les terminaux s'en trouve diluée.

Notamment en ce qui concerne les usages professionnels, la question de la maîtrise des terminaux mobiles est pourtant fondamentale. De ce point de vue, et en raison de la prolifération des outils d'attaques qui se déploient sur les plateformes mobiles, il est fondamental de séparer les usages personnels et professionnels.

La sécurité de la couche radio n'est qu'un des nombreux aspects que revêt la sécurité des réseaux cellulaires. L'accroissement des performances des terminaux mobiles et de leurs moyens de communication promet une multiplication des usages qu'il est impératif de sécuriser. Ainsi, l'ouverture de la carte USIM, élément de confiance des terminaux, à des applications tierces requiert une vigilance particulière. Dans une autre mesure, son remplacement prévisible par des implémentations logicielles reposant sur des fonctions de cloisonnement des processeurs telles que ARM/TrustZone nécessite également des précautions. Plus généralement, la maîtrise des terminaux par les usagers est un élément fondamental de la sécurité ; cette maîtrise plaide en faveur d'une ouverture accrue des systèmes exécutés au sein des terminaux.

Références

1. Airprobe GSM sniffing. `https://svn.berlin.ccc.de/projects/airprobe/`.
2. OpenBSC. `http://openbsc.osmocom.org/`.

3. OpenBTS : An opensource telephone network. http://bipinb.com/openbts-an-opensource-telephone-network.htm.
4. OsmocomBB. http://bb.osmocom.org/.
5. The Kraken. http://srlabs.de/research/decrypting_gsm/.
6. GNU Radio. http://gnuradio.org/redmine/wiki/gnuradio, 1998.
7. 3GPP. 3G Security ; Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS ; Document 1 : A5/3 and GEA3 specifications (TS 55.216). http://www.3gpp.org/ftp/Specs/html-info/55216.htm.
8. 3GPP. 3G Security ; Specification of the A5/4 Encryption Algorithms for GSM and ECSD, and the GEA4 Encryption Algorithm for GPRS (TS 55.226). http://www.3gpp.org/ftp/Specs/html-info/35226.htm.
9. 3GPP. 3G Security ; Specification of the MILENAGE algorithm set : An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5* ; Document 2 : Algorithm specification (TS 35.206). http://www.3gpp.org/ftp/Specs/html-info/35206.htm.
10. 3GPP. Characteristics of the Universal Subscriber Identity Module (USIM) application (TS 31.102). http://www.3gpp.org/ftp/Specs/html-info/31102.htm.
11. 3GPP. Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (TS 51.014). http://www.3gpp.org/ftp/Specs/html-info/1114.htm.
12. 3GPP. Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface (TS 51.011). http://www.3gpp.org/ftp/Specs/html-info/1111.htm.
13. 3GPP. Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (TS 31.111). http://www.3gpp.org/ftp/Specs/html-info/31111.htm.
14. Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of gsm encrypted communication. In *CRYPTO*, 2003.
15. Alex Biryukov, Adi Shamir, and David Wagner. Real Time Cryptanalysis of A5/1 on a PC. In *International Workshop on Fast Software Encryption*, 2000.
16. Orr Dunkelman, Nathan Keller, and Adi Shamir. A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony. Cryptology ePrint Archive, Report 2010/013, 2010. http://eprint.iacr.org/.
17. Patrik Ekdahl and Thomas Johansson. Another Attack on A5/1. In *IEEE Transactions on Information Theory*, 2002.
18. Tobias Engel. Locating Mobile Phones using SS7. 25th Chaos Communication Congress, 2009.
19. Commission Nationale Informatique et Liberté. Les applications de géolocalisation sur mobile en questions. http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/les-applications-de-geolocalisation-sur-mobile-en-questions/, 2010.
20. ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2 : ZUC Specification. Technical report, ETSI, 2011. http://www.gsmworld.com/documents/EEA3_EIA3_ZUC_v1_5.pdf.

21. ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4 : Design and Evaluation Report. Version 1.3, 18th January 2011. Technical report, ETSI, 2011. http://www.gsmworld.com/documents/EEA3_EIA3_Design_Evaluation_v1_3.pdf.
22. European Information Technology Observatory. More than five billion mobile phone users. http://www.eito.com/pressinformation_20100811.htm, 2010.
23. Grugq. Base Jumping – Attacking the GSM Baseband and Base Station. Blackhat Abu Dhabi, https://media.blackhat.com/bh-ad-10/Grugq/BlackHat-AD-2010-Gurgq-Base-Jumping-slides.pdf, 2010.
24. Xavier Lagrange, Philippe Godlewski, and Sami Tabbane. *Réseaux GSM*. 2000.
25. Karsten Nohl and Luca Melette. GPRS Intercept : Wardriving your country. Chaos Communication Camp, 2011.
26. Karsten Nohl and Sylvain Munaut. Wideband GSM sniffing. 27th Chaos Communication Congress, 2010.
27. Karsten Nohl and Chris Paget. Gsm - srlsy ? In *26th Chaos Communication Congress*, 2009.
28. Orange. Couverture réseau en france. http://couverture-reseau.orange.fr/france/netenmap.php.
29. SFR. Couverture réseau en france. http://assistance.sfr.fr/mobile_forfait/mobile/couverture-reseau/en-48-62267.
30. Bruno Sido. Rapport d'information sur la couverture du territoire en téléphonie mobile. http://www.senat.fr/rap/r10-348/r10-3481.pdf, 2011.
31. Dieter Spaar. A practical DoS attack to the GSM network. DeepSec, 2009.
32. Bouygues Télécom. Couverture réseau en france. http://www.cartographie.bouyguestelecom.fr/eCouverture/eCouverture.aspx.
33. Ralf-Philipp Weinmann. All Your Baseband Are Belong To Us – over-the-air exploitation of memory corruptions in GSM software stacks. Laboratory for Algorithmics, Cryptology & Computer Security University of Luxembourg https://cryptolux.org, 2010.
34. Harald Welte. OsmocomBB - A tool for GSM protocol level security. In *SSTIC*, 2010.