Extrait du Spyworld Actu

http://www.spyworld-actu.com/spip.php?article12500

« En pratique, attaquer Kasumi n'est pas réalisable sur les GSM »

- Technologie -

Date de mise en ligne : mercredi 20 janvier 2010

Spyworld Actu

Selon Hervé Sibert, expert en sécurité, les hypothèses requises par l'attaque sur les clés de chiffrement GSM utilisées ne sont jamais vérifiées.

Mercredi dernier la rédaction publiait un article concernant une attaque supposée casser l'algorithme de chiffrement GSM A5/3. Hervé Sibert, expert en cryptographie s'est rapproché de la rédaction pour apporter un niveau de précision supplémentaire : « Pour réussir l'attaque en question qui vise Kasumi, bloc constituant d'A5/3, il faut réussir à avoir un contrôle presque total des entrées et sorties de ce bloc. » Selon lui, si les détails de l'attaque sur le bloc ne sont pas remis en cause, une analyse en profondeur est nécessaire afin de déterminer l'impact sur l'algorithme A5/3 utilisé en 2G, et sur les autres algorithmes de sécurité GSM utilisant le bloc Kasumi : UEA1 en 3G (UMTS), et GEA3 en GPRS. Hervé Sibert en est arrivé à la conclusion que l'attaque n'est pas applicable en pratique. « Mieux, ajoute-t-il, dans le cas de A5/3 et GEA3, les hypothèses requises par l'attaque sur les clés utilisées ne sont strictement jamais vérifiées. »

01netPro : Peut-on dire que Kasumi est synonyme d'A5/3 ?

Hervé Sibert : Non. Kasumi est une brique utilisée dans les algorithmes de chiffrement GSM A5/3 (2G), UEA1 (3G) et GEA3 (GPRS) (voir schéma ci-dessous).

Quelle est l'utilisation de Kasumi dans A5/3, UEA1 et GEA3 ?

On applique Kasumi à des données publiques (connues) en utilisant une clé dérivée de la clé de session CK (dérivée de manière pseudo-aléatoire dans la SIM à partir d'une donnée de 128 bits provenant du réseau) pour obtenir une graîne pseudo-aléatoire (étape non représentée sur le schéma).Une suite de blocs de masquage S est ensuite générée de manière itérative en appliquant Kasumi avec la clé CK : un bloc de masquage est généré en chiffrant le XOR du bloc de masquage précédent, d'un compteur incrémenté à chaque bloc et de la graîne pseudo-aléatoire. Enfin, les blocs de masquage S sont utilisés pour masquer (par XOR) les blocs de données M (voix encodée par exemple) avant transmission sur l'interface radio.

Quel est le but de l'attaque ?

Elle vise à récupérer quatre clés de session CK différentes utilisées pour générer des blocs de masquage.

Quelle est la pertinence de cette attaque ?

L'attaque publiée doit remplir trois conditions :
1 - Choisir plusieurs mégaoctets de données à faire chiffrer par Kasumi. Ceci est impossible puisque ces données sont bien définies et hors du contrôle d'un attaquant,
2 - Capturer les millions de blocs de masquage S correspondant, ce qui revient à connaître tous les blocs de données M, en pratique impossible à moins de s'introduire dans le mobile. Mais alors à quoi bon casser le chiffrement si on peut accéder aux données en clair avec un cheval de Troie ?
3 - Les quatre clés de session que l'on souhaite retrouver doivent être liées mathématiquement : elles doivent se déduire les unes des autres en changeant le 33e et/ou le 97e bit. Les clés de session sont générées de manière pseudo-aléatoire hors du contrôle d'un attaquant, donc attendre qu'elles vérifient ce genre de relation est du même ordre de complexité qu'une attaque par recherche exhaustive (force brute).

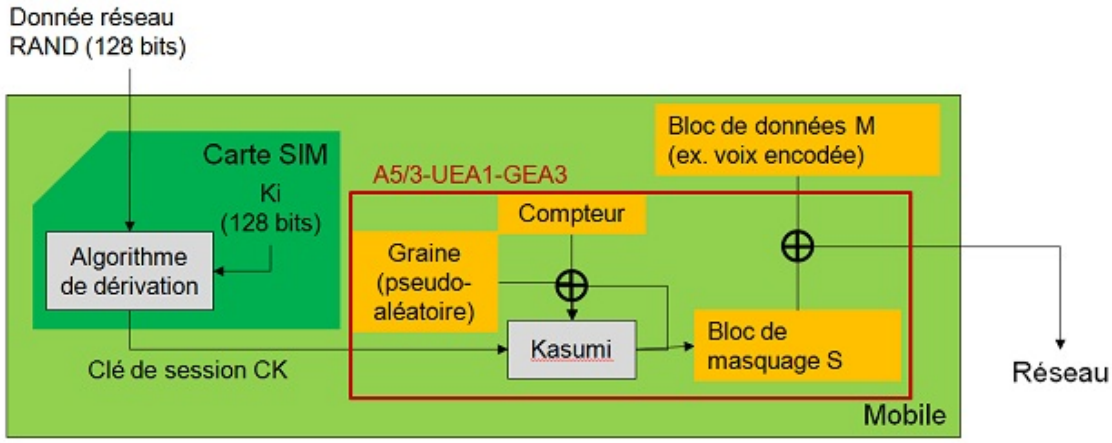
Cette attaque n'est donc pas utilisable en pratique étant donné la manière dont est utilisé Kasumi dans le GSM. A noter que, dans A5/3 et GEA3, les spécifications détaillées forcent les 33ème et 97ème bits de chaque clé à être identiques. Par conséquent, jamais un ensemble de clés répondant aux besoins de l'attaque ne sera utilisé.

Quel est le statut des algorithmes GSM après cette attaque ?

Les algorithmes 2G A5/2 et A5/1 sont cassés, et ceci depuis longtemps (bien avant les annonces de décembre 2009 sur A5/1). Cette nouvelle attaque ne permet pas de casser A5/3, UEA1 ou GEA3 plus efficacement qu'une attaque par recherche exhaustive. Elle a même une probabilité de succès absolument nulle contre A5/3 et GEA3. Il est intéressant de noter que de nombreux algorithmes de chiffrement sont vulnérables à des « related-key attacks » sans que cela ne pose de véritable menace en pratique.

Des algorithmes à la sécurité accrue sont utilisés dans les nouveaux standards (4G/LTE) ou introduits dans des standards existants (2G, 3G). Ainsi, l'algorithme SNOW 3G est la base de LTE et est en cours d'introduction dans le standard 3G UMTS (UEA2), et il est probable qu'une version 2G voie le jour rapidement. LTE permettra aussi l'usage du standard AES. Enfin, la 2G verra bientôt l'utilisation de clés de 128 bits dès l'algorithme A5/4, au lieu de 64 bits actuellement. Le GSM se prépare donc à parer des attaques qui, elles, seraient exploitables en pratique contre A5/3, UEA1 et GEA3.

Le processus de chiffrement



Algorithme de dérivation : algorithme qui, à partir d'une donnée RAND et de la clé de l'abonné Ki, génère une clé de session de manière pseudo-aléatoire (c'est-à-dire sans biais statistique).

Graine pseudo-aléatoire : valeur générée par une étape d'initialisation en appliquant Kasumi à un bloc de 64 bits connu, en utilisant une clé différente de CK

Compteur : nombre de blocs générés (incrémenté après chaque bloc)

Bloc de masquage : les blocs de 64 bits générés par Kasumi sont appelés blocs de masquage (ou suite chiffrante) car ils sont utilisés pour masquer bit par bit les blocs de données à chiffrer. A réception des blocs masqués,

l'infrastructure réseau connaît la clé CK utilisée et peut donc générer les mêmes blocs de masquage pour démasquer les données.

Post-scriptum :

http://pro.01net.com/editorial/5113...