



Panorama de la Cybercriminalité

Alain Thivillon – CTO

Hervé Schauer Consultants

<http://www.hsc.fr/>

La sécurité du GSM compromise ?

Trois évènements de ce début 2010

- 29/12/2009 : au Chaos Computer Congress (Berlin), annonce d'avancées majeures dans le cassage du chiffrement GSM, par pré-calcul distribué sur des cartes graphiques, code source public
- 31/12/2009 : Record battu pour le calcul des décimales de PI (2700 Milliards), par un effort individuel (131 jours de calcul sur un seul PC, 7To de stockage)
- 8/01/2010 : Annonce par l'INRIA (et d'autres) de la factorisation d'une clé RSA 768 Bits : 30 mois de calcul par 1500 CPU

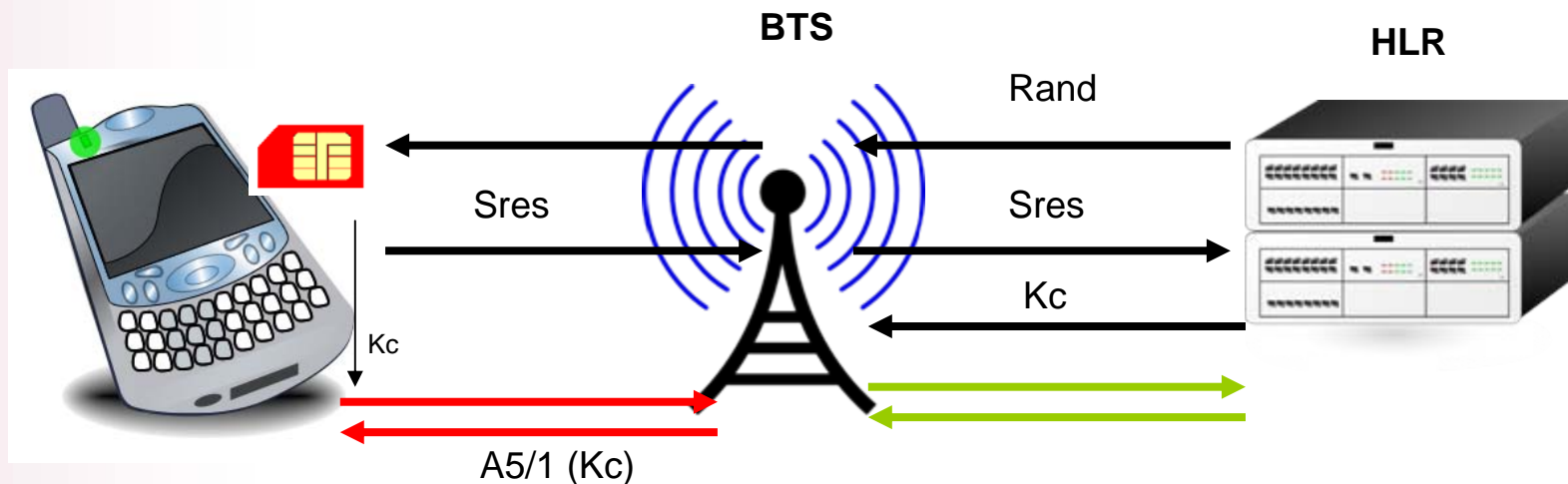
La loi de Moore (et l'intelligence des algorithmiciens et cryptologues) à l'œuvre : les puissances de CPU et de stockage permettent des calculs cryptographiques jugés hier réservés à des gouvernements.

Chaos Computer Congress (CCC)

- Congrès de « hackers » en Allemagne (Berlin)
 - 26^e édition cette année (26C3)
<http://events.ccc.de/congress/2009/>
 - Ne concerne pas seulement la sécurité informatique : vie privée, « building things », « Net Activism », ...
- Evènement non commercial
 - Beaucoup moins d'auto-censure qu'à BlackHat
 - Entrée ~ 100 euros
- Déjà connu pour des annonces sur la sécurité
 - Cassage RFID
 - Cassage Xbox

La sécurité GSM (2G)

Authentification et Confidentialité reposent sur les secrets contenus dans la SIM de l'abonné et dans le réseau opérateur, desquels sont dérivés une clé de chiffrement symétrique utilisée dans un algorithme nommé A5/1 (chiffrement Radio).



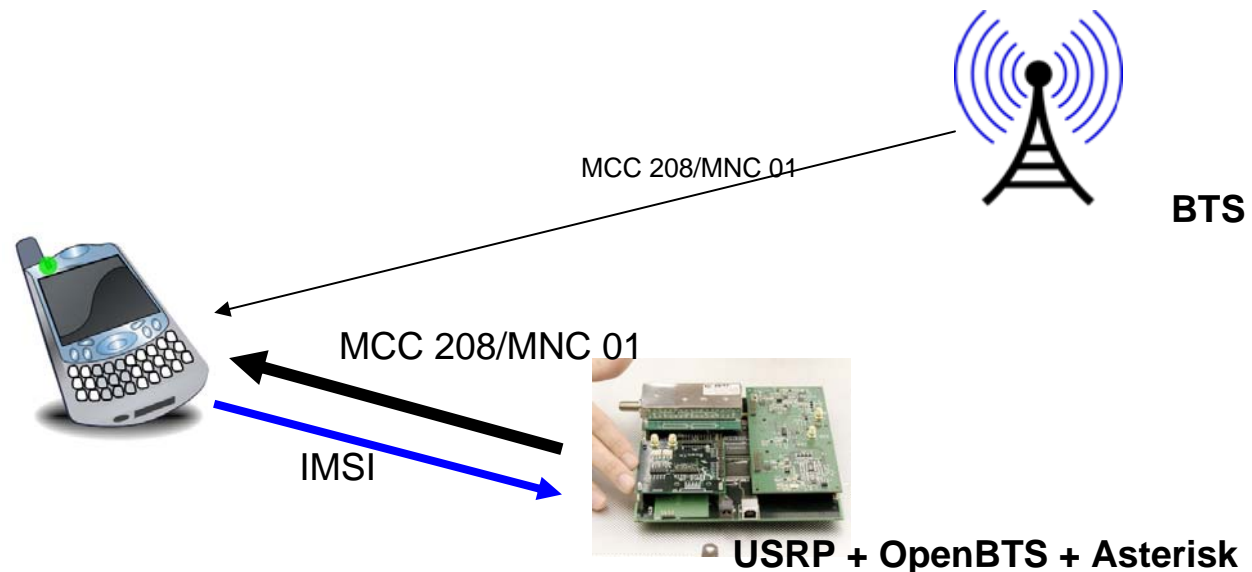
A5/1

- Algorithme conçu en 1987
 - Pas public, reverse-engineeré en 1997
 - Attaques théoriques publiées depuis cette date, mais peu d'impact pratique public
 - En 2008, THC a commencé à publier du code puis a fait disparaître le projet (pressions ?)
- A5/2 est un autre algorithme dégradé « export »
 - Cassable en quelques millisecondes
 - Le réseau choisit le chiffrement
- Manque d'authentification mutuelle
 - Le téléphone ne peut pas authentifier le réseau

Attaque « active »

• Utilisation d'une fausse BTS

- Projet « OpenBTS » OpenSource + USRP (Décodeur/Encodeur Radio)
- Connecté au réseau téléphonique par Asterisk (GSM → SIP)
- Permet de tester aussi la solidité du téléphone GSM, dénis de service, ...
- Passage en A5/2 et craquage immédiat (utilisé par les solutions commerciales)



Attaque « passive »

- Le temps de calcul d'un dictionnaire complet A5/1:
 - 100000 ans d'un CPU classique
 - 128 Péta-Octets de stockage
- Karsten Nohl (DE), cryptologue
 - Déjà connu pour le reverse-engineering et le cassage de RFID mifaire
 - Reprise du travail de THC
- Utilisation de techniques nouvelles
 - Amélioration des algorithmes et portage sur GPU (Cartes graphiques Nvidia et ATI)
 - Utilisation de « Rainbow Tables » permettant de restreindre l'espace de stockage tout en gardant un temps de calcul raisonnable

Attaque « passive » - 2

• Résultats

- Utilisation de 40 GPU en calcul distribué pendant 3 mois
- Rainbow Tables totales de 2To représentant 99% de l'espace de clés

• Conséquences

- Récupération de la clé de chiffrement d'une conversation assez longue et décryptage en quelques minutes
- Possibilité de déchiffrer avec 50% de probabilité la signalisation (SMS, ...) même sans conversation

• La partie la plus dure est de « sniffer » le mobile

- Gestion des sauts de fréquence
- Utilisation de USRP2 (~2500\$)
- Encore du travail pour faire un produit « tous terrains »



Réaction GSM Association

A hacker would need a radio receiver system and the signal processing software necessary to process the raw radio data. The complex knowledge required to develop such software is subject to intellectual property rights, making it difficult to turn into a commercial product.

...

Moreover, intercepting a mobile call is likely to constitute a criminal offence in most jurisdictions.

Puisque la sécurité est mauvaise, changeons de cible de sécurité ...

Et après ? ...

- Réseaux 3G
 - SIM → USIM
 - Utilisation d'autres algorithmes (KASUMI)
 - Authentification mutuelle !
- Réseaux 2G
 - Passage encouragé depuis longtemps à A5/3 (Dérivé des algorithmes 3G)
 - Contraintes opérateurs fortes (fiabilité, charge des réseaux, compatibilité, ...)
 - Ca n'empêche pas l'attaque MITM et la dégradation d'algorithme ...
- Kasumi cassé ?
 - Faiblesses connues
 - Nouveau papier hier ! (signé par SHAMIR/RSA)
 - Résistance dans 5 ou 10 ans ... ?

URLS

Conférence CCC (slides + Video) :

<http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html>

Karsten Nohl : <http://reflexor.com/trac/a51>

GSM Association : <http://www.gsmworld.com/newsroom/press-releases/2009/4490.htm>

INRIA/RSA 768 : <http://www.inria.fr/actualites/espace-presse/cp/pre210.fr.html>

2700 Milliards de décimales de PI, Fabrice Bellard :

<http://bellard.org/pi/pi2700e9/>

Attaque « Sandwich » sur Kasumi :

<http://eprint.iacr.org/2010/013>