
DEF CON
DEF CON 18

Avant propos : Vie privée

- Intercepter des appels téléphoniques
- Eteindre les téléphones pour votre vie privée
- Données non concernés :
  - Le BTS est en mode live
- Améliorer les nombres des victimes

C’est quoi l’IMSI ?

- IMSI=International Mobile Subscriber Identity
- Une des identifications de la carte SIM
  - Analogie au nom de la carte SIM
- Dans la carte SIM
- TMSI identifiant en Um

C'est quoi l'IMSI-Catcher?

- Les fausses stations de base
- Signal élevé
  - Les pirates gagnent dans tous les cas
- En GSM, priorité du BTS
  - A5/x ; Puissance Tx, Gain Rx
- Signal élevé + A5/0 => Obtention Victimes
- Première apparition en 1993 par R&S
  - Que pensez vous de notre pays ?

IMSI-CATCHER crypto

- L'attaquant et son BTS malicieux
- Connexion des victimes dans le BTS
- BTS sans chiffrement
- Obtention des victimes sans rainbowtable

- Avertissements possibles mais:
  - Trop de confusion des utilisateurs
  - Par défaut, message désactivé par l'opérateur

Les Spectres utilisées

- 4 bandes pour le réseau GSM
  - 850, 900, 1800, 1900
- GSM-850 et GSM-1900 utilisés en USA
  - 900 et 1800 en Europe
- 900 et 1800 en Europe
- US ISM Band : 902-928Mhz
  - Quelques fois 902-914Mhz
- Quand-Bande supporte ISM-Bande
  - Les téléphones en Europe également

ISM Bande

- Industrial , Scientific, Medical band
  - Basse puissance et Basse fréquence
- Peut-on utiliser ISM band pour le GSM!?
  - La réponse et oui!

Amateur Radio

- Facilité d’avoir du License
  - http://kb0mga.net/exams pour l'examen
  - Bien comprendre les questions
- 1500W puissance limite (!)
- Transmission numérique possible à condition :
  - Une spécification publique
- Pas de Chiffrement
- Pas de limitation sur l’ antenne
- Vérification de fréquence toutes les 10minutes

Identifier le BTS

- Utilisation de BTS avec plus de puissance
- Configuration égale à l'opérateur dans GSM

  -> Self-Dos
- Besoin de script en 900Mhz

ID-Me

- Une introduction sur IM-ME
  - Travis Good speed a fait le travail
  - http://travisgoodspeed.blogspot.com/2010/03/im-me-goodfet-wiring-tutorial.html
- +10dbm en sortie, large bande de fréquence
- Facile à programmer en C
  - Flashage par Travis's GoodFET
- fréquence ⇔ puissance de l'USRP
- Amplification du signal

Installation du BTS

- USRP
  - 2xRFx900
  - ClockTamer
    - http://code.google.com/p/clocl-tamer
    - précisions de l'horloge (+/-100Hz en 1.9Ghz)
- Laptop
  - Debian
  - OpenBTS
  - Asterisk
- Un BTS GSM : voix seulement

Demo 1

BTS en test Mode

Cloner l'opérateur

- Identification Réseau : MCC et MNC
- Mobile Country Code (310 pour USA)
  - Listes en Wikipedia
- Mobile Network Code (2-3 digits)
  - Listes en Wikipedia
- Pour un changement :
  - Cloner le réseau GSM selon MCC et MNC
- Vérification par la carte SIM
  - Nom sensible à la casse par certains opérateurs

Demo 2

Cloner MNC/MCC
Nom de l’opérateur

Perspective

- DIY IMSI-Catcher
  - Capture du victime dans la station de base
- Possibilité d'ajout filtre IMSI-IMEI
  - IMEI = Identifiant de l'Equipement
- Cette technique prend beaucoup du temps
  - Comment la procéder rapidement ?
- Capture des appels et SMS entrant seulement
  - Comment procède t-on pour les trafics sortants ?

Handover plus rapide

- Que faire pour avoir plus de victime ?
  - Comment le faire plus rapidement ?

- Beaucoup de possibilités
- Le Neighbours List
- Changement de LAC
- Utilisation de Brouilleur
- Amélioration de gain Rx

GSM-Neighbours

- Listes de station voisine
  - Partage des canaux à utiliser
- Monitoring des canaux voisins
  - Augmentation la rapidité de handover
- L'attaquant utilise ses infos pour :
  - Identifier les cellules voisines
  - Installer la station de base
  - Interconnecter rapidement les téléphones du BTS

Les cellules voisines

- Nokia 3310(900/1800) / 3390(1900)
  - Network monitor mode
  - Un renifleur (sniffer) de GSM aux alentours
- Utilisation de FBUS et MBUS Câble
- Utilisation de Gammu
  - Interprétation de wireshark
- Utilisation de liste voisine par la signalisation « System Information 2 »

Demo 3

Net Monitoring avec Location area Code

Local Area Code

- Envoie du LAC dans la broadcaste par le BTS
- Groupe de cellules pour une zone définie
  - Handover facile
- Changement de LAC …
  - … Changement de nouvelle zone
  - … Téléphone en mode Handover
- Changement de LAC -> Rapidité handover

Demo 4

Changement du LAC

Puissance

- Pas de connaissance de paramètres pour la première fois de la station
  - Les fréquences et les LAC
- Long scan évité par
  - MNC et MCC avec haut signal
- Scan rapide dans ce cas

- Perte du signal, même procédé
  - Avantageux pour l'attaquant

Perte des signaux

- Concernant 2G
  - Bonne conception pour 3G
- Jamming 2G
  - Moyen facile pour trouver des victimes
- Jamming 3G
  - Interception 3G difficile
  - Attaque pour forcer les victimes à utiliser 2G
- Peut-on créer un jammer sur toute la bande ?

Générateur de bruit

- l'attaquant peut transmettre bruit puissant
  - Un signal perturbateur pour la cellule
  - Une perte de signal pour les victimes
- Le générateur de bruit est-il chers ?
  - 450 dollars en eBay
- L'amplificateur de puissance est-ils chers ?
  - 400dollars pour 100watt
- 100w de bruit = grande perturbation

Demo 5

Brouilleur des réseaux cellulaires

Juste pour rire

- Dangerosité des brouilleurs de réseau mobile
  - GSM, CDMA, 3G, 4G …
- Impossible de défendre contre eux
- Besoin de quelques burst seulement
  - Un moyen de faire l'attaque plus offensive
- Jusqu'où le Dos se propage-t-il?
  - Avec 100w et une bonne antenne!
  - Dos tous Las Vegas
  - Qu'est ce qui va se passer après ?

Rx Gain

- Astuce du BTS
  - Envoi du signal en usurpant sa mesure comme X dbm
- Configuration définie par la spécification GSM
  - Options à compléter dans certains cas
- Bonne configuration du BTS selon l'attaquant
  - Inexistante commande pour OpenBTS
- point essentiel trouvé par R&S compagnie

Inbound Call

- IMSI-Catcher ⇔ cellule séparée
  - Téléphone éteint pour les services entrants
- téléphone éteint -> Voice mail
  - Que peut on faire d'autres ?
- Résultat :

l'attaquant n'a pas les services entrants

- Solution : faire un spoofing du réseau

Les problèmes du spoofing

- Connaissance de l’IMSI/IMEI
  - Pas forcément la connaissance de Ki

- connecter avec l'IMSI de la victime
- Envoyer RAND challenge de victime
- Casser key Stream de la victime
- Découvrir la clé de session kc
- Réutiliser cette clé

Casser la clé de session?

- Avoir besoin de casser un crypto
  - Comme amélioration de l'IMSI-Catcher
- Négociation de la cryptographie utilisée
  - A5/2 idéal pour être craqué
  - A5/1 nécessite un rainbowtable
- Pas de chiffrement pour les outban

Solutions : ??

- Pas dans le contexte de GSM – GSM est mort
- Beaucoup de pays avec des mauvais config
  - Implémentation de crypto diffèrent
- Première solution : Utilisation du 3G
  - Non encore craqué de nos jours
- Deuxième solution : Plus de chiffrement
  - Comme avec Internet; chiffrement à la source
- Meilleure solution : Eteindre 2G utilise 3G …