État des lieux de la Sécurité des réseaux cellulaires

Chaouki Kasmi et Benjamin Morin

ANSSI

Conférence C&ESAR
29 novembre 2011

Plan

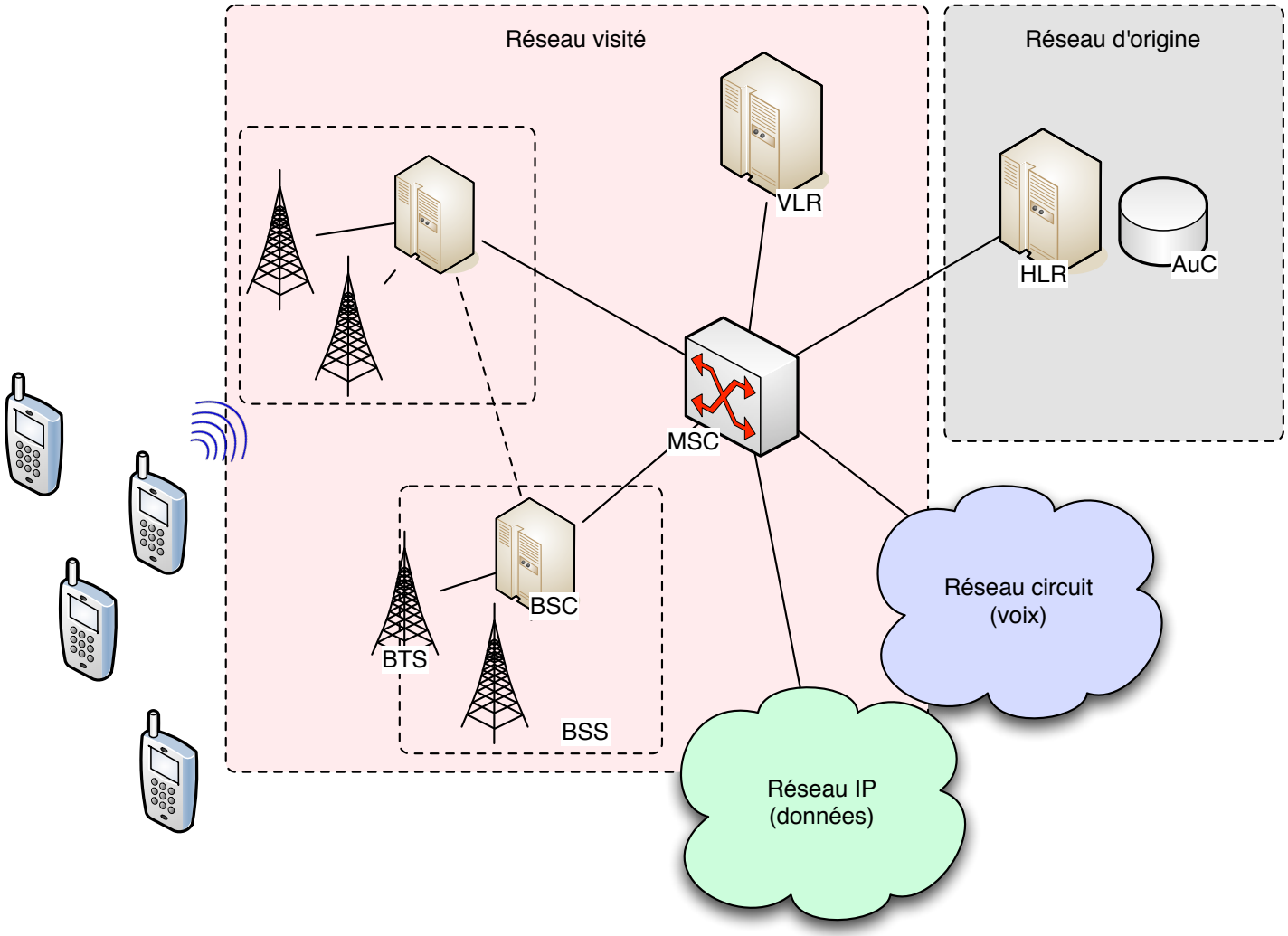
Contexte

- Les réseaux de communication cellulaires sont apparus au début des années 90
  - Principes de conception relativement opaques
  - Pratiques de développement datant parfois de plusieurs années
- Les technologies et usages qui reposent sur ces réseaux ne se cantonnent plus à la téléphonie et évoluent très vite
  - Évolution des terminaux : smartphones, tablettes, PC, etc.
  - Évolution des domaines : transport, énergie, etc.
- Plusieurs études indépendantes ont récemment mis en lumière des vulnérabilités dans ces réseaux
  - Projets communautaires de développement d'outils d'analyse
  - Matériel accessible à moindre coût
  - Mise en pratique d'attaques réputées théoriques

Motivations

- Les réseaux cellulaires doivent plus que jamais satisfaire des exigences de sécurité
  - Confidentialité des communications
  - Intégrité des communications et des équipements
  - Disponibilité / résilience des réseaux
- Cette présentation se concentre sur la sécurité des réseaux cellulaires
  - État de l'art des avancées récentes en matière d'analyse des éléments constitutifs d'un réseau cellulaire
  - Protocoles et équipements intervenant au niveau de la couche radio
  - Problèmes de géolocalisation
- Cette présentation n'aborde pas (ou peu) la sécurité de la partie applicative des terminaux
  - Ce thème est un sujet d'étude à part entière
  - Nombreux projets et publications à ce sujet

Architecture d'un réseau cellulaire



Plan

Contexte

- Le secteur de la mobilité est en plein essor
  - Applications innombrables
  - Multiplication des terminaux dits « intelligents »
  - Ouverture du secteur à de nouveaux acteurs
  - L'engouement suscité par la mobilité pose de nombreux problèmes de sécurité
- Multitude de parties prenantes dans ce secteur
  - Opérateurs, fabricants de terminaux, développeurs, utilisateurs, ...
  - Les exigences de sécurité des acteurs sont difficiles à concilier
- Pose le problème de la maîtrise des terminaux
  - L'ouverture des terminaux est partielle
  - Le fonctionnement de plusieurs sous-systèmes demeure opaque
  - La maîtrise des terminaux est diffuse
  - La confiance dans le matériel et le logiciel embarqué dans les terminaux est-elle justifiée ?

Architectures de terminaux mobiles

- Cohabitation de plusieurs environnements d'exécution
  - Environnement « applicatif » (système d'exploitation et applications utilisateur)
  - *Baseband* (communications radio)
  - Contrôleurs de périphériques
  - Carte (U)SIM
- Surface d'attaque importante
  - Applications malveillantes
  - Vulnérabilités des systèmes d'exploitation ou des applications
  - Attaques contre le *baseband*
  - Attaques des couches basses (bluetooth, NFC) et hautes (Wi-fi)
- Nécessité d'isoler ces environnements d'exécution
  - Doit empêcher un élément malveillant d'interférer avec les environnements d'exécution tiers
  - L'isolation peut être logique ou physique
- Identification de l'équipement : IMEI supposé unique et non-modifiable

Cartes (U)SIM (*(Universal) Subscriber Identity Module*)

La carte SIM est l'élément de sécurité des terminaux

- Élément fondamental de la sécurisation des communications
  - Protection de clés cryptographiques et d'identifiants du porteur (IMSI/TMSI)
  - Exécution d'algorithmes d'authentification et de dérivation de clés
  - Accès protégé par le code PIN du porteur
- Sous le contrôle des opérateurs
- Ouverture progressive à des applications tierces (type NFC)

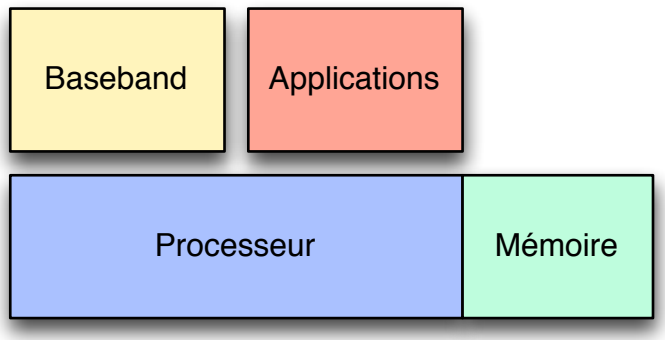
Projets d'étude associés

- Projet SIMTrace (attaque « par le milieu »)
- Analyse des échanges entre le réseau et la carte SIM
  - Acquisition des échanges (AT+C et RESP) entre la carte (U)SIM et le Base-band
  - Etudes du fonctionnement : protocole de communication T0 et recherche de commandes non-documentées

Baseband

- Composant responsable des communications radios (interface air, modem)
  - Pile protocolaire :
    - L1 : couche physique
    - L2 : couche liaison - LAPDm
    - L3 : couche de gestion de mobilité, de connexion et des ressources radios
  - 70% du marché détenu par trois constructeurs : Qualcomm, Infineon et Texas Instrument
  - Architecture ARM à 60%
  - Utilisé en boite noire par les fabricants d'équipements mobiles
  - Mise à jour à distance par le fabricant du modem au travers des infrastructures d'opérateur de téléphonie mobile

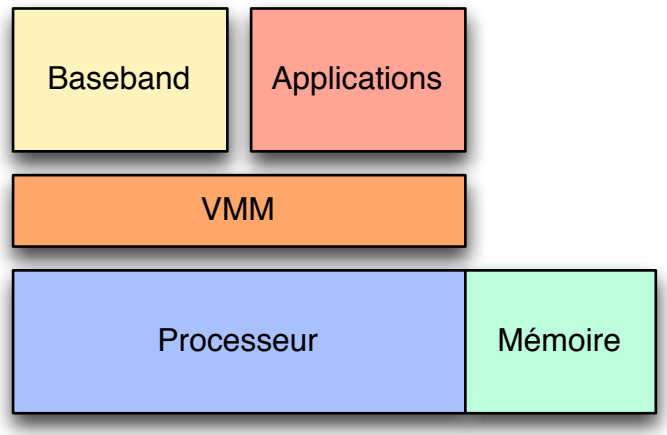
- Différents modes d'intégration dans les terminaux
  - Processeur dédié ou partagé
  - Mémoire dédiée ou partagée



Baseband

- Composant responsable des communications radios (interface air, modem)
  - Pile protocolaire :
    - L1 : couche physique
    - L2 : couche liaison - LAPDm
    - L3 : couche de gestion de mobilité, de connexion et des ressources radios
  - 70% du marché détenu par trois constructeurs : Qualcomm, Infineon et Texas Instrument
  - Architecture ARM à 60%
  - Utilisé en boite noire par les fabricants d'équipements mobiles
  - Mise à jour à distance par le fabricant du modem au travers des infrastructures d'opérateur de téléphonie mobile

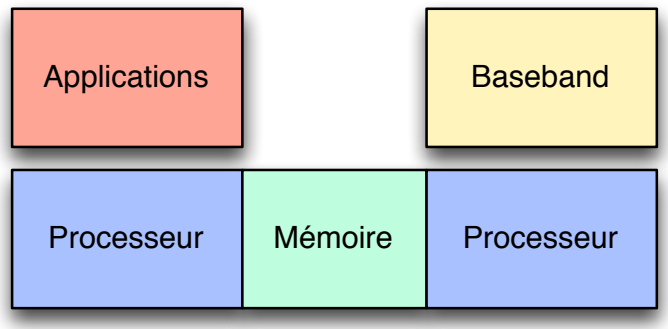
- Différents modes d'intégration dans les terminaux
  - Processeur dédié ou partagé
  - Mémoire dédiée ou partagée



Baseband

- Composant responsable des communications radios (interface air, modem)
  - Pile protocolaire :
    - L1 : couche physique
    - L2 : couche liaison - LAPDm
    - L3 : couche de gestion de mobilité, de connexion et des ressources radios
  - 70% du marché détenu par trois constructeurs : Qualcomm, Infineon et Texas Instrument
  - Architecture ARM à 60%
  - Utilisé en boite noire par les fabricants d'équipements mobiles
  - Mise à jour à distance par le fabricant du modem au travers des infrastructures d'opérateur de téléphonie mobile

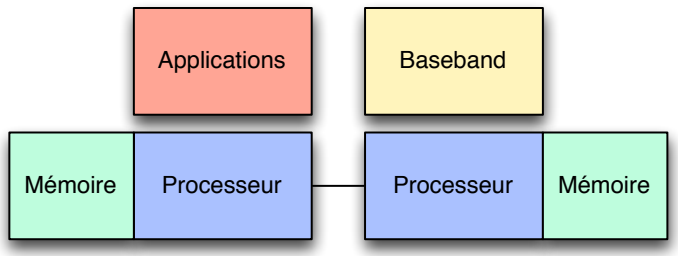
- Différents modes d'intégration dans les terminaux
  - Processeur dédié ou partagé
  - Mémoire dédiée ou partagée



Baseband

- Composant responsable des communications radios (interface air, modem)
  - Pile protocolaire :
    - L1 : couche physique
    - L2 : couche liaison - LAPDm
    - L3 : couche de gestion de mobilité, de connexion et des ressources radios
  - 70% du marché détenu par trois constructeurs : Qualcomm, Infineon et Texas Instrument
  - Architecture ARM à 60%
  - Utilisé en boite noire par les fabricants d'équipements mobiles
  - Mise à jour à distance par le fabricant du modem au travers des infrastructures d'opérateur de téléphonie mobile

- Différents modes d'intégration dans les terminaux
  - Processeur dédié ou partagé
  - Mémoire dédiée ou partagée

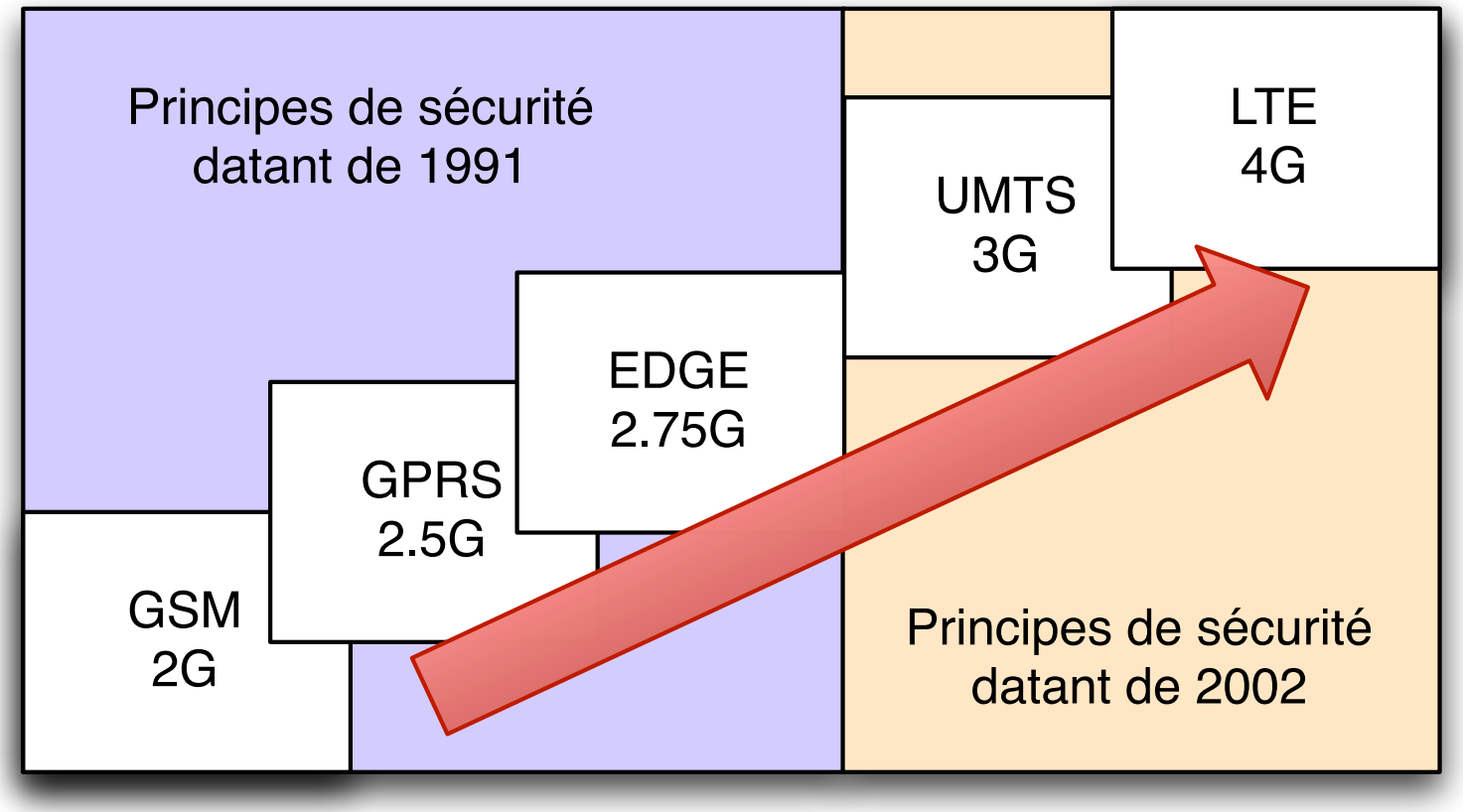


Baseband

- Menaces associées au *baseband*
  - Principe de conception opaque
  - Vulnérabilités logicielles
  - Absence de protections standards
- Conséquences d'une prise de contrôle du *baseband* ?
  - Attaque du réseau cellulaire (7, 11)
  - Extension de la prise de contrôle au domaine applicatif du terminal (12)
- Des audits de sécurité de ces composants sont nécessaires afin d'évaluer leur robustesse
- Projets associés
  - OsmocomBB (4) et OpenMoko : implémentation logicielle ouverte d'un *baseband*
  - OpenBTS (3) : *fuzzers* de *baseband*

Plan

Évolution des standards



Couches PHY et MAC des réseaux mobile

- Réseau de type cellulaire
- Interface radiofréquence full duplex utilisant TDD [1] et FDD [2]
- Modulation GMSK, OFDM, utilisation de codes correcteurs
- Trois bandes de fréquence (900 MHz, 1800 MHz, 2100 MHz)
- Utilisation du saut de fréquence en fonction de la charge de l'antenne-relais
- Choix de l'algorithme cryptographique pour la gestion de la confidentialité imposé par le réseau

1. Time-Division Duplexing
2. Frequency-Division Duplexing

Protection des communications GSM, GPRS, EDGE

Authentification

- Authentification unilatérale du terminal v-à-v du réseau
- Algorithme A3 (non normalisé) exécuté par la carte SIM avec une clé K_i

Protection des communications GSM, GPRS, EDGE

Authentification

- Authentification unilatérale du terminal v-à-v du réseau
- Algorithme A3 (non normalisé) exécuté par la carte SIM avec une clé K_i

L'absence d'authentification du réseau par le terminal permet des attaques par le milieu

Protection des communications GSM, GPRS, EDGE

Authentification

- Authentification unilatérale du terminal v-à-v du réseau
- Algorithme A3 (non normalisé) exécuté par la carte SIM avec une clé K_i

L'absence d'authentification du réseau par le terminal permet des attaques par le milieu

Chiffrement

- Dérivation d'une clé de chiffrement K_c avec l'algorithme A8
- Communications chiffrées par le terminal jusqu'à l'antenne-relais
- Famille d'algorithmes de chiffrement symétriques
  - A5/1, A5/2 (export), A5/3, A5/4 (issus de Kasumi) et GEA.

Protection des communications GSM, GPRS, EDGE

Authentification

- Authentification unilatérale du terminal v-à-v du réseau
- Algorithme A3 (non normalisé) exécuté par la carte SIM avec une clé K_i

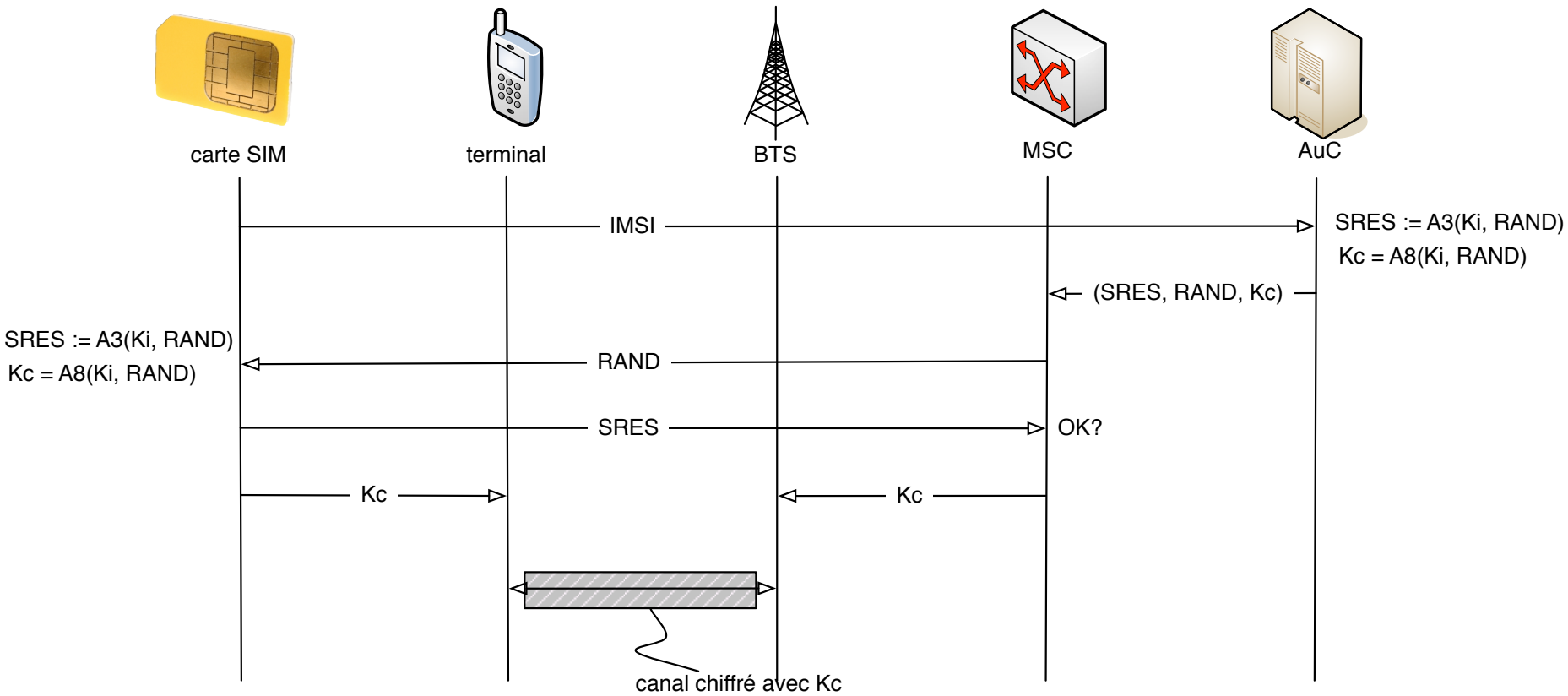
L'absence d'authentification du réseau par le terminal permet des attaques par le milieu

Chiffrement

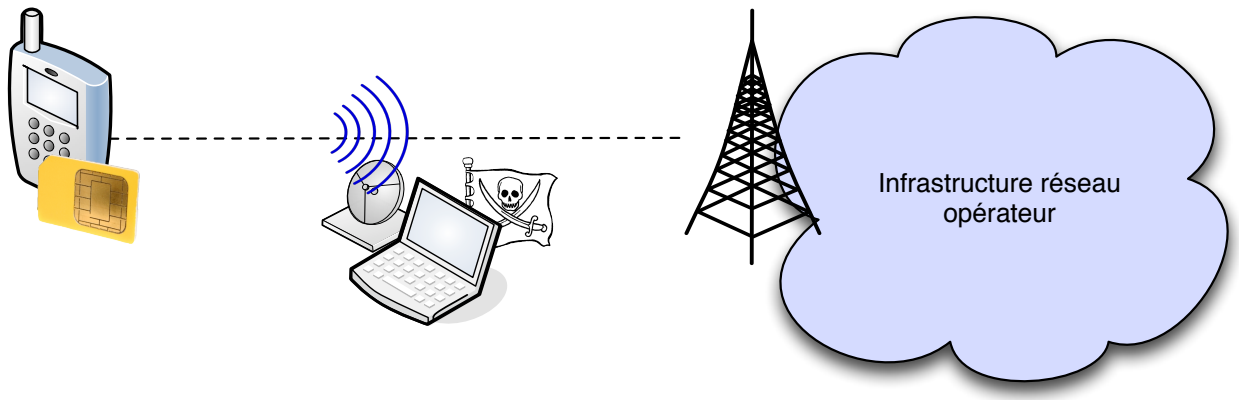
- Dérivation d'une clé de chiffrement K_c avec l'algorithme A8
- Communications chiffrées par le terminal jusqu'à l'antenne-relais
- Famille d'algorithmes de chiffrement symétriques
  - A5/1, A5/2 (export), A5/3, A5/4 (issus de Kasumi) et GEA.

Des attaques pratiques contre les algorithmes A5/1 et A5/2 permettent des écoutes passives des communications (10)

Protection des communications GSM, GPRS et EDGE

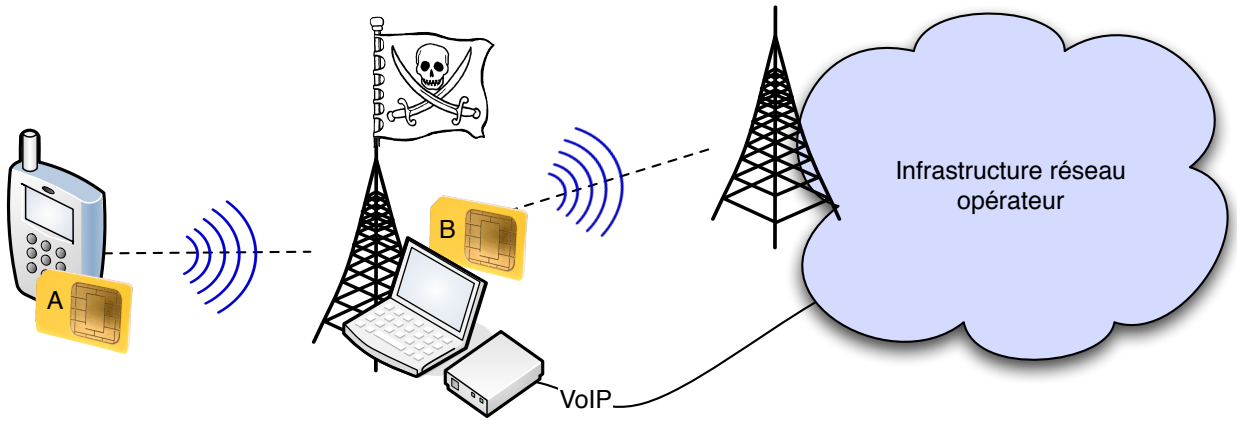


Attaque passive de l'interface air



- Réalisation des écoutes facilitée par l'apparition de la radio logicielle (6)
- Projets et outils associés
  - The Kraken (5)
  - AirProbe (1)

Attaque active de l'interface air



- Projets et outils associés
  - OpenBTS
  - OsmocomBB
  - BTS commerciales + OpenBSC
  - Utilisation malveillante d'une femtocell (8)

Protection des communications 3G et 4G

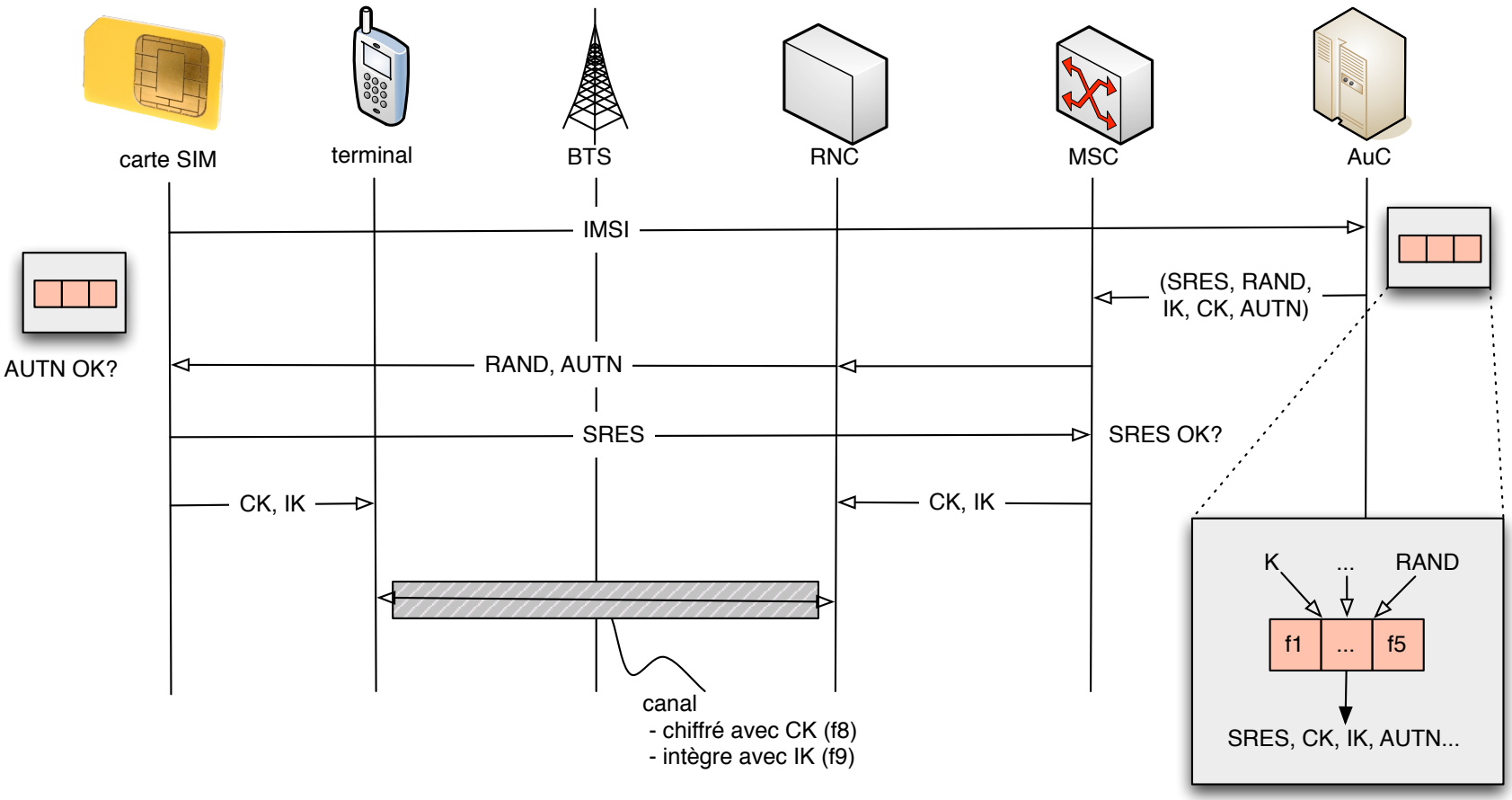
Authentification

- Authentification mutuelle du réseau et de l'abonné
- Exemple d'algorithme : Milenage (fondé sur AES)

Chiffrement et intégrité

- Collection de fonctions de dérivation de clés f_i
- Algorithmes de chiffrement Kasumi et Snow3G (+ Zuk ?)
- Chiffrement des communications prolongé au sein du réseau de l'opérateur (RNC)

Protection des communications 3G et 4G



Conclusion sur les protocoles de communication

Les réseaux de nouvelle génération (3G, LTE) améliorent significativement la sécurité des communications

- Authentification mutuelle du réseau et du terminal
- Utilisation d'algorithmes robustes

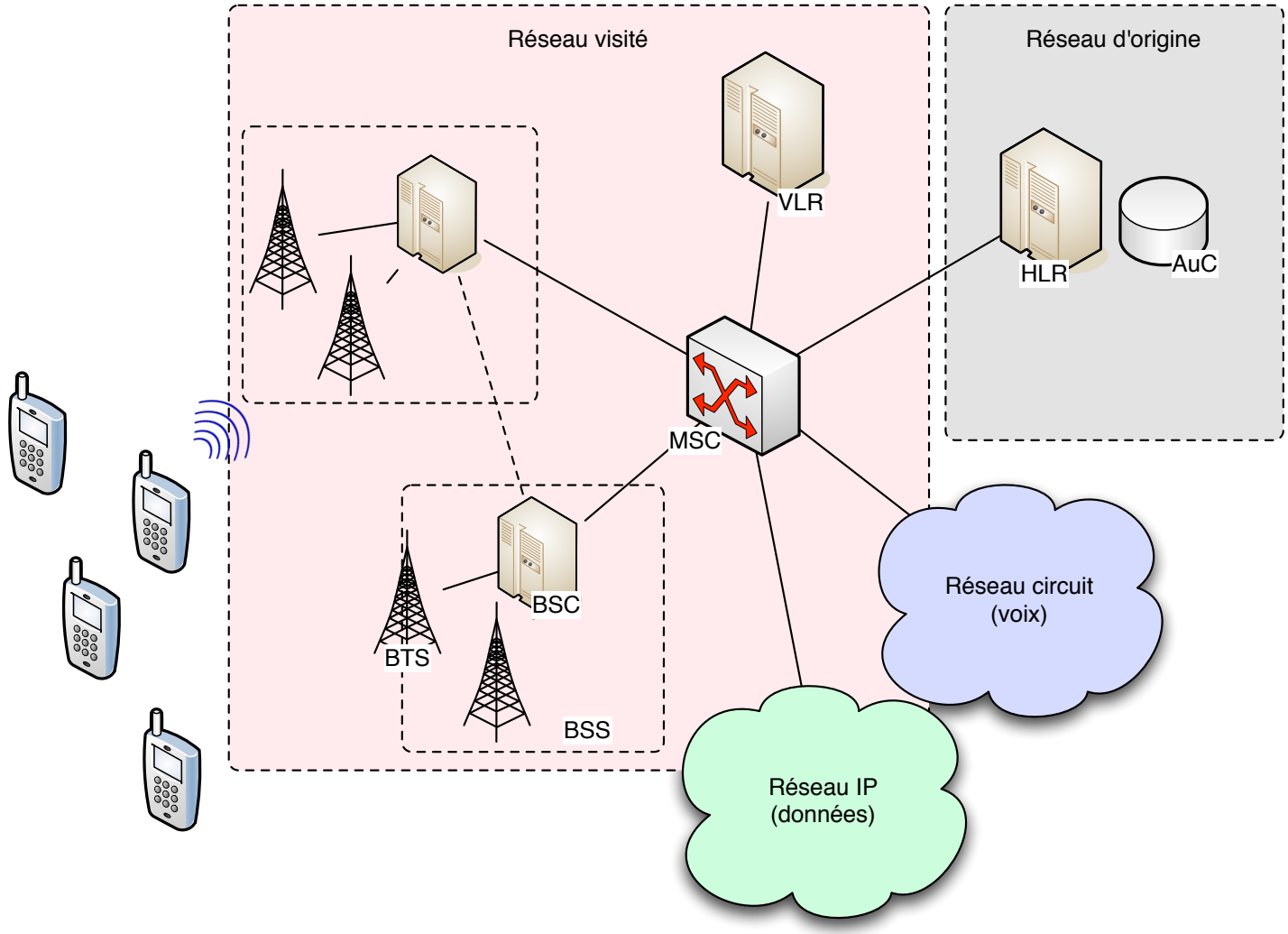
Mais leur couverture demeure inférieure à celle des réseaux d'ancienne génération (GSM, GPRS, EDGE)

- Il est nécessaire de pousser l'utilisation de l'algorithme A5/3
- Empêche *a minima* les interceptions passives
- Le problème des attaques actives demeure

Attention au déploiement d'équipement de résilience radio non sécurisé donnant l'accès aux mécanismes cryptographiques

Plan

Architecture type



Equipements d'infrastructure 1/2

- Le réseau compte plusieurs types d'équipements :
  - BTS(2G)/ Node-B(3G) : antenne-relais, point d'accès réseau
  - BSC(2G)/ RNC(3G) : contrôleur de station de base, gestion des ressources radios
  - MSC : routeur réseau, routage des données dans l'infrastructure d'opérateur
  - VLR/HLR : base de donnée conservant les informations des abonnées
  - AuC : équipement de gestion des mécanismes d'authentification
- Les spécifications techniques de ces équipements sont très complexes et les implémentations sont spécifiques aux constructeurs (certaines spécifications ne sont pas respectées)

Equipements d'infrastructure 2/2

- Analyse du fonctionnement de ces équipements par un tiers :
  - Approche pratique : test d'équipement impossible, les infrastructures sont suivies de façon drastique (pas partout)
  - Approche théorique : conception et réalisation d'équipement par exploitation des spécifications, difficile car certaines spécifications ne sont pas publiques (NDA)
- Implémentation et test par exploitation de document technique à disposition et par rétro-conception d'équipements achetés dans des pays où la gestion d'infrastructure est moins drastique

Projets

- Station de base GSM/GPRS : OpenBTS (3),
- Contrôleur de station de base : OpenBSC (2),
- Implémentation d'un système d'exploitation et d'un *baseband* : OpenMoko et OsmocomBB (4)
- Implémentation des protocoles de signalisation : OpenSS7
- Passerelle GPRS (interface entre Internet et le réseau mobile) : OpenGGSN

Droit et protection de la vie privée

Article 226-15 du code pénal, De l'atteinte au secret des correspondances

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

Plan

Applications et intérêts liés à la géolocalisation

- Les applications de la géolocalisation sont nombreuses, deux catégories :
  - Applications utiles
  - Applications nuisibles portant atteinte au respect de la vie privée
- Les données de géolocalisation sont l'objet de convoitise
  - Par les développeurs d'applications et de systèmes d'exploitation
  - Pour les fournisseurs de services via ces acteurs (Ex. publicité ciblée)
- Accès aux données de géolocalisation
  - L'accès et la divulgation de données permettant la géolocalisation des utilisateurs doit recueillir leur consentement explicite
  - Les exceptions à cette règle sont strictement encadrées
- Les moyens de géolocaliser un terminal sont nombreux
  - Puces GPS
  - Gestion de la mobilité dans le réseau

Gestion de la mobilité dans un réseau cellulaire

Qui dispose des informations de positionnement dans le réseau ?

- L'opérateur
  - Routage des appels et des données
  - Statut du terminal (éteint/allumé)
- Le terminal de l'abonné
  - Au moins trois antennes-relais à disposition (Cell ID)
  - Gestion du *handover*

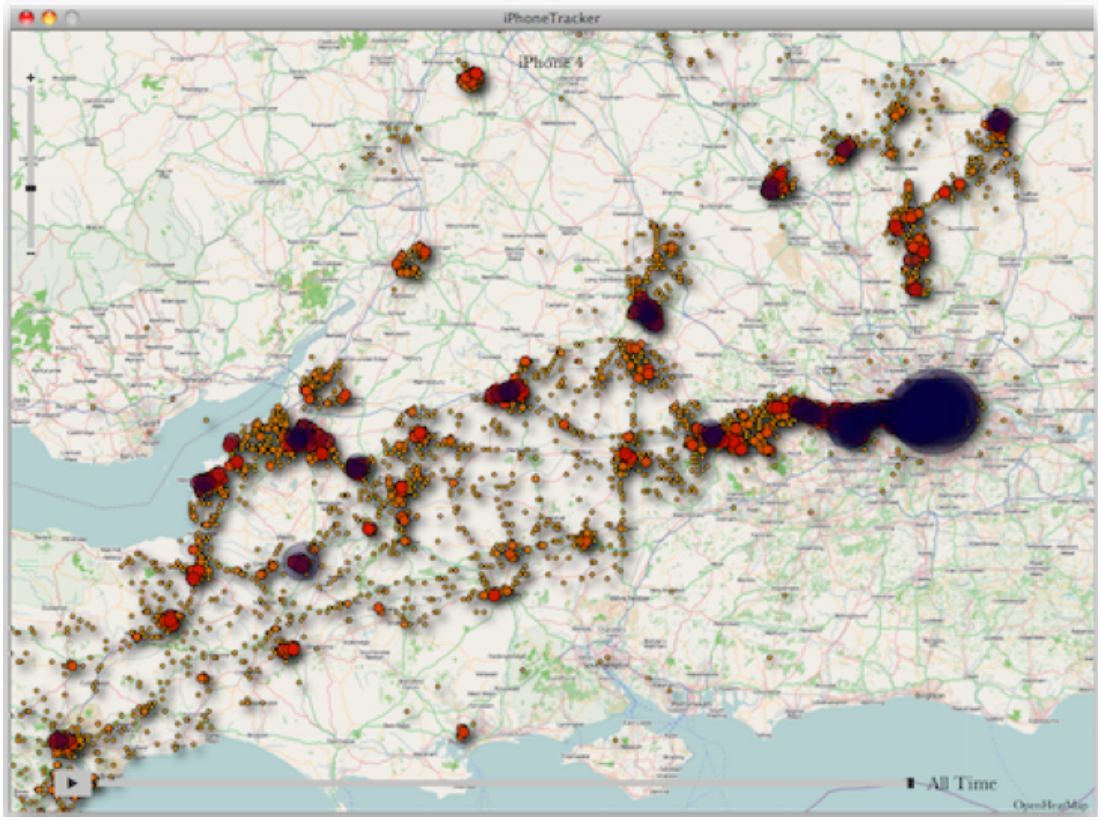
Géolocalisation à distance et suivi d'individu

- Géolocalisation à distance
  - La compromission d'un équipement par la diffusion d'application malveillante
  - Installation d'application demandant l'accès à ces informations
- Suivi d'un individu avec une station de base
  - Nécessite la connaissance de l'IMSI de l'individu (possible pour 0.01/€ HLR-Look'up) et une cartographie du réseau
  - Récupération de l'IMSI, du dernier TMSI et de l'IMEI possible

Projets de cartographie

Plusieurs projets visent à alimenter des bases de données (Cell ID ↔ position GPS)

- Techniques de *wardriving* (9)
- Projets communautaires (OpenCellId, crowdflow)
- Systèmes de géolocalisation brevetés par Apple et Google



Plan

Conclusion

- L'étude de la sécurité des réseaux cellulaires est restée confidentielle pendant longtemps
- Plusieurs projets ouverts d'analyse de ces réseaux ont émergé ces dernières années
  - Ces projets ont permis de mettre en évidence des problèmes de sécurité
  - Leur utilisation doit rester encadrée pour limiter les utilisations malveillantes
- Les réseaux de nouvelle génération améliorent notablement la situation
- Mais la confiance dans les terminaux reste limitée
  - Des efforts de sécurisation notables ont été faits (essentiellement au niveau de l'environnement applicatif)
  - Le problème de la maîtrise des terminaux par les utilisateurs demeure
- Il est nécessaire de renforcer la sécurité des terminaux mobiles
  - Notamment concernant les nouveaux usages (NFC, ...)

Bibliographie I

(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) Chaouki Kasmi et Arnaud Ebalard ANSSI. *Radio logicielle : impact sur la SSI.* CE&SAR 2011.

(7) 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.

(8) Jean-Pierre Seifert. *Femtocells security.* CE&SAR 2011.

(9) Karsten Nohl and Luca Melette. *GPRS Intercept : Wardriving your country.* Chaos Communication Camp, 2011.

(10) Karsten Nohl and Chris Paget. *Gsm - srlsy ?* In *26th Chaos Communication Congress*, 2009.

(11) Dieter Spaar. *A practical DoS attack to the GSM network.* DeepSec, 2009.

(12) 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.