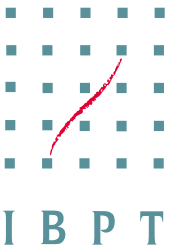

INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS

AVIS DU CONSEIL DE L'IBPT DU 17 FÉVRIER 2012 AU MINISTRE VANDE LANOTTE CONCERNANT LES RISQUES POTENTIELS D'ATTEINTE À LA SÉCURITÉ DES RÉSEAUX ET SERVICES DE TÉLÉPHONIE MOBILE DANS LE CADRE DES TECHNOLOGIES 2G ET 2.5 G

Version à destination du public

Institut belge des services postaux et des télécommunications
Ellipse Building - Bâtiment C - Boulevard du Roi Albert II 35 - 1030 Bruxelles
Tél. 02 226 88 88 Fax 02 226 88 77 http://www.ibpt.be

TABLE DES MATIÈRES

EXECUTIVE SUMMARY

Le Ministre Johan Vande Lanotte, Vice-Premier Ministre et Ministre de l'Economie, des Consommateurs et de la Mer du Nord , a demandé à l'IBPT de faire état de la sécurité des réseaux et services belges de téléphonie mobile. L'IBPT a répondu à cette demande dans un avis du 17 février 2012.

L'avis de l'IBPT se fonde sur une analyse interne ainsi que sur une enquête qu'il a menée auprès des principaux fournisseurs de services de téléphonie mobile GSM, GPRS et EDGE sur base des articles 113 et 114 de la loi du 13 juin 2005 relative aux communications électroniques.

La dite enquête de l'IBPT révèle qu'aucun élément tangible ou soupçon de violation de la sécurité n'a pu être confirmé pour l'ensemble des opérateurs.

L'IBPT aboutit à la conclusion que la sécurité des réseaux et services est aujourd'hui satisfaisante mais peut être améliorée. De par les mesures qui ont déjà été adoptées et celles qui sont programmées, les opérateurs démontrent une réelle volonté d'atteindre rapidement un niveau plus élevé de sécurité.

Finalement, l'IBPT a déjà planifié une nouvelle analyse globale au quatrième trimestre de l'année 2012. Cette analyse globale comprendra une analyse interne, une nouvelle enquête auprès des opérateurs ainsi que des contrôles sur l'efficacité de la sécurité des réseaux GSM, GPRS et EDGE.

1. CONTEXTE ET OBJET DE L'AVIS

1.1. Développements récents

De récentes publications ont souligné plusieurs vulnérabilités potentielles au sein des services de téléphonie mobile. Différents groupes d'experts ont en effet annoncé des progrès majeurs en cryptologie[1] et proposent également de nouvelles solutions matérielles ainsi que des logiciels qui permettraient de pirater les communications sur les réseaux mobiles.

Les recherches les plus médiatisées sont celles réalisées par un expert allemand, Monsieur Karsten NOHL. En décembre 2009, son équipe et lui-même ont proposé des tables de recherche optimisées pour casser l'algorithme de chiffrement A5/1 et annoncé la démonstration prochaine de solutions permettant de contourner les protections des réseaux de téléphonie mobile. En août 2011, il a dévoilé les ressources matérielles et les logiciels qui, selon lui, seraient suffisants pour y parvenir et en décembre 2011, il a publié une étude concernant 31 opérateurs de téléphonie mobile[2]. Cette étude conclut notamment que toutes les mesures ne sont pas prises par les opérateurs belges pour assurer le plus haut niveau de sécurité. Trois aspects de la sécurité y sont critiqués : l'usurpation d'identité, la localisation de l'usager et l'espionnage des communications.

Il est difficile d'adhérer *a priori* purement et simplement à des travaux dont les motivations, la méthodologie et les résultats ne sont pas clairement explicités et qui manquent de la nécessaire transparence requise pour toute démonstration scientifique.

[1] La cryptologie est la science mathématique qui étudie les méthodes permettant d'échanger des informations de manière confidentielle.
[2] http://gsmmap.org/

En outre, il s'agit d'un avis émanant d'un seul expert. Néanmoins, cette étude a le mérite d'attirer l'attention sur des vulnérabilités potentielles au sein des technologies de téléphonie mobile 2G et 2.5G.

A l'inverse, depuis décembre 2009, la «GSM Association» (GSMA)[3], qui regroupe les opérateurs de téléphonie mobile et les entreprises connexes à travers le monde, défend une position rassurante concernant la matière de la sécurité. Elle répond aux publications de l'équipe NOHL par le communiqué de presse suivant :

«[…] Reports of an imminent GSM eavesdropping capability are common. The GSMA, which welcomes research designed to improve the security of communications networks, routinely monitors the work of groups in this area. […] before a practical attack could be attempted, the GSM call has to be identified and recorded from the radio interface. So far, this aspect of the methodology has not been explained in any detail and we strongly suspect that the teams attempting to develop an intercept capability have underestimated its practical complexity. 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. […][4]»

A notre connaissance, la GSMA ne s'est pas prononcée sur les dernières publications de l'équipe NOHL.

1.2. Objet de l'avis

Le 27 décembre 2011, Monsieur le Ministre Johan Vande Lanotte, Vice-Premier Ministre et Ministre de l'Economie, des Consommateurs et de la Mer du Nord, a demandé à l'IBPT d'enquêter sur les risques potentiels d'atteinte à la sécurité des services belges de téléphonies mobiles.

L'IBPT a ainsi mené une enquête auprès des principaux fournisseurs belges de services de téléphonie mobile GSM, GPRS et EDGE concernant les risques potentiels d'atteinte à la sécurité des services de téléphonie mobile. Cette enquête consista en une dynamique d'échanges entre les opérateurs et l'IBPT sur les mesures actuelles et futures que les opérateurs belges ont prises ou prendront afin de garantir l'intégrité et la confidentialité de leurs services GSM, GPRS et EDGE. Une attention particulière a été également portée à la sécurité des messageries vocales.

En ce début d'année 2012, l'IBPT a ainsi interrogé les principaux fournisseurs de services de téléphonie mobile 2G et 2.5G, en l'occurrence Belgacom, Mobistar et KPN Group Belgium, en leur soumettant un questionnaire relatif à la gestion actuelle et future de la sécurité de leur réseau mobile et aux risques d'atteinte à cette dernière.

Les informations récoltées étant de nature confidentielle, elles ne peuvent être révélées en tant que telles dans le présent document.

Après avoir évoqué le cadre juridique (point 2) et après avoir justifié la limitation aux technologies 2G et 2.5G (point 3), la présente note expose la position des opérateurs (point 4), l'analyse interne de l'IBPT quant à la problématique des risques d'atteinte à la sécurité des

[3] Ses missions consistent essentiellement à soutenir le développement et la promotion du réseau GSM ainsi que les technologies qui en sont dérivées.

[4] GSMA - GSMA Statement on Media Reports Relating to the Breaking of GSM Encryption. Communiqué de presse du 30 décembre 2009. http://www.gsma.com/newsroom/.

services de téléphonie mobile (point 6), l'analyse des réponses des opérateurs (point 7) et émet finalement des conclusions (point 8).

2. CADRE JURIDIQUE

Sur base des articles 113 et 114 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après dénommée la loi du 13 juin 2005), l'IBPT dispose de compétences en matière de sécurité des réseaux et services publics de communications électroniques. L'article 114 précité prévoit entre autres ce qui suit :

> *«Le fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de communications électroniques en ce qui concerne la sécurité du réseau. Compte tenu de l'état de la technique et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.*
> *[…]Lorsqu'il existe un risque particulier d'atteinte à la sécurité de son réseau, l'opérateur concerné informe les abonnés et l'Institut de ce risque.*
> *[…]Lorsqu'il constate une atteinte à l'intégrité de son réseau, l'opérateur concerné prend toutes les mesures nécessaires afin d'informer dans les plus brefs délais les autorités, les opérateurs et les abonnés concernés.»*

En outre, l'article 14, §1er, 3°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges, dite loi-statut, charge l'IBPT de contrôler le respect de la loi du 13 juin 2005.

L'enquête susmentionnée fut dès lors menée sur base de ces dispositions.

Enfin, c'est sur base de l'article 14, § 1er, 1°, de ladite loi-statut que l'IBPT a émis l'avis au Ministre Johan Vande Lanotte.

3. PORTÉE LIMITEE DE L'AVIS AUX TECHNOLOGIES 2G ET 2.5G – EXCLUSION DES TECHNOLOGIES 3G ET ULTÉRIEURES

Le présent avis se limite aux services de téléphonie mobile 2G et 2.5G, ci-après dénommés «réseaux mobiles» et se focalise particulièrement sur la sécurité des communications sur la voie radio, c'est-à-dire entre le terminal de l'usager (un téléphone portable par exemple) et les infrastructures du réseau.

3.1. Les technologies 2G et 2.5G

Pour rappel, les télécommunications mobiles sont passées de réseaux basés sur des normes analogiques, dits de «première génération» - dans les années 80, aux capacités restreintes et incompatibles entre elles - vers des réseaux basés sur une norme GSM[5].

[5] GSM : *Global System for Mobile Communications* - Système global pour les communications mobiles

L'innovation essentielle des réseaux GSM, GPRS et EDGE par rapport aux technologies de téléphonie mobile précédentes[6] est leur caractère entièrement numérique. Celui-ci apporte une amélioration indéniable des performances (meilleure exploitation des ressources spectrales et régénération de l'information par exemple) et a naturellement conduit au succès que cette génération de réseaux connaît depuis 1991, soit plus de 20 ans. Lors de l'élaboration de ces normes, la sécurité des communications n'avait néanmoins pas l'importance qui lui est accordée aujourd'hui et elle se basait sur des mécanismes qui peuvent être remis en cause au regard des progrès technologiques récents.

Le réseau GSM est la seconde technologie de téléphonie mobile, dite «2G», qui supporte entre autres le transfert de la voix et l'échange de courts messages textuels (SMS) par commutation de circuits.

Le réseau GPRS[7] est une technologie dérivée du réseau GSM, qui introduit le transfert de données par commutation de paquets. Elle est généralement qualifiée de technologie « 2.5G ».

Enfin, le réseau EDGE[8] est une amélioration des réseaux précédents et permet essentiellement d'atteindre des débits de transferts plus importants.

3.2. Les technologies 3G et ultérieures

La troisième génération (3G) de technologies de téléphonie mobile et les technologies ultérieures proposent d'atteindre des débits supérieurs à ceux des réseaux 2G ou 2.5 ouvrant ainsi la porte à des usages multimédias tels que la transmission de vidéo, la visioconférence ou l'accès à internet haut débit. L'élaboration des normes 3G et de générations ultérieures bénéficient de l'expérience acquise, notamment en matière de sécurité, de sorte que ces nouvelles technologies bénéficient de mécanismes de protection plus matures, plus complexes et plus performants que ceux repris dans le cadre du 2G et du 2.5G[9]. L'analyse de ce réseau n'est dès lors pas comprise dans le présent avis.

4. POSITION DES OPERATEURS

De manière générale, les opérateurs considèrent que la sécurité fait partie intégrante du développement de leur réseau mobile et le démontrent par la désignation de personnel affecté exclusivement à cette charge et par les investissements consentis dans ce domaine.

Les opérateurs argumentent que la sécurité de leur réseau mobile est efficace mais sont aussi conscients que le niveau de sécurité devra augmenter en fonction de l'évolution de la menace, et grâce aux nouvelles fonctionnalités qui sont dorénavant disponibles. Ils soulignent que toute évolution de leur système ne peut s'effectuer qu'après des phases de tests et de validation poussées et qu'ils doivent évaluer non seulement leur pertinence, les coûts qui y sont associés et le temps nécessaire à leur mise en œuvre, mais surtout l'impact de ces mesures sur l'expérience

[6] La première génération 1G de téléphonie mobile repose sur des communications analogiques et regroupe plusieurs standards, notamment les réseaux *Nordic Mobile Telephone* (NMT), *Advanced Mobile Phone System* (AMPS), *Total Access Communication System* (TACS) ou encore Radiocom 2000.
[7] GPRS : *General Packet Radio Service* – Service de transfert de données en commutation de paquets.
[8] EDGE : *Enhanced Data Rates for GSM Evolution* - Débit de données enrichi pour l'évolution globale.
[9] Les normes 3G proposent notamment des clés en 128 bits, une authentification mutuelle et une signalisation cryptée.

de l'usager. Il s'agit selon eux d'assurer la compatibilité de leurs nouvelles solutions avec les terminaux les plus anciens.

Sur base des informations obtenues des opérateurs, l'IBPT reconnaît les efforts consentis par ces derniers pour atteindre un haut niveau de sécurité de leur réseau mobile.

De par les mesures qui ont déjà été prises et qui ont été programmées, les opérateurs font preuve d'implication en démontrant une réelle volonté d'accroître la sécurité de leur réseau mobile et de rapidement converger vers cet objectif.

5. ANALYSE INTERNE

5.1. Sécurité des réseaux mobiles

L'analyse interne de l'IBPT est basée sur l'état de l'art de la sécurité des réseaux mobiles. Cet état de l'art expose les mécanismes de sécurité et les confronte aux standards actuels du point de vue des vulnérabilités, des menaces et des contre-mesures.

Les enjeux majeurs en matière de sécurité des services de téléphonie mobile sont les suivants :

- les communications et les activités de l'usager ne doivent pas être accessibles à un quelconque tiers ;
- un usager doit pouvoir en permance être identifié de manière unique sur le réseau de l'opérateur ;
- seul l'usager peut accéder aux services auxquels il a souscrit.

Le risque d'atteinte à la sécurité est lié au niveau actuel de menace, qui augmente du fait des prouesses technologiques, face à la vulnérabilité des réseaux mobiles. Si ce risque d'atteinte est avéré, il s'agirait alors de prendre les mesures nécessaires pour réduire le niveau de vulnérabilité des réseaux mobiles.

Les vulnérabilités les plus critiques des réseaux mobiles sont inhérentes à leur architecture de sécurité et ne sont donc pas nouvelles. En effet, lors de l'élaboration des spécifications GSM, l'objectif primordial était de proposer une technologie de téléphonie mobile entièrement numérique et unanimement approuvée. Aujourd'hui, il faut remettre en question l'absence d'authentification mutuelle et l'utilisation de certains algorithmes de chiffrement qui sont devenus désuets au regard des avancées technologiques.

L'analyse interne de l'IBPT montre que le suivi systématique et le déploiement des nouvelles fonctionnalités, telles que celles introduites par les organismes de normalisation, permettent de minimiser les risques d'atteinte à la sécurité des réseaux mobiles.

5.2. Contraintes liées à une hausse du niveau de sécurité

Une hausse du niveau de sécurité ne doit pas s'effectuer aux dépens de l'expérience du client et des capacités opérationnelles des opérateurs. Un compromis est donc indispensable. Par ailleurs, la compatibilité des terminaux belges et étrangers doit être étudiée avant d'appliquer une nouvelle mesure de sécurité.

6. ANALYSES DES RÉPONSES DES OPÉRATEURS

Les réponses des opérateurs sont confidentielles et ne peuvent donc être transmises dans le présent avis.

L'analyse réalisée par l'IBPT se limite volontairement à une évaluation qualitative et globale du risque d'atteinte à la sécurité. La portée des vulnérabilités et des contre-mesures associées n'a pas été considérée en termes de facteurs d'impact tels que le nombre d'usagers affectés. L'IBPT ne peut dès lors quantifier de façon précise le risque d'atteinte à la sécurité.

L'analyse montre néanmoins que les opérateurs prennent, de leur propre initiative, des mesures en vue d'assurer un haut niveau de sécurité de leurs réseaux mobiles. Ils étudient et planifient à l'heure actuelle de nouvelles mesures pour accroître encore davantage le niveau de sécurité de leurs réseaux mobiles.

En matière de sécurité, les réseaux mobiles sont en mutation et il serait inopportun d'investir aujourd'hui dans une analyse plus détaillée, qui ne serait plus valable demain. L'IBPT envisage donc d'attendre le dernier quadrimestre 2012 que la sécurité des réseaux se stabilise avant de poursuivre une analyse plus approfondie. L'IBPT restera vigilant à ce que les mesures annoncées aujourd'hui deviennent effectives.

7. CONCLUSIONS FINALES

Dans le cadre de l'enquête, les opérateurs n'ont communiqué à l'IBPT aucun élément qui pourrait mener l'IBPT à conclure en une violation de la sécurité de leurs réseaux mobiles.

L'IBPT remarque que les opérateurs témoignent d'une attention particulière envers la sécurité de leur réseau mobile en termes de gestion, d'investissements et de veille technologique. *A priori*, la sécurité de leur réseau mobile est aujourd'hui satisfaisante. Elle peut toutefois être améliorée en implémentant notamment les dernières fonctionnalités délivrées par les spécifications des normes GSM, GPRS et EDGE.

L'IBPT effectuera une nouvelle analyse globale au quatrième trimestre de l'année 2012.
Cette analyse globale comprendra une analyse interne complémentaire, une enquête plus large auprès des opérateurs ainsi que des contrôles sur l'efficacité de la sécurité des réseaux mobiles.

Axel Desmedt
Membre du Conseil

Charles Cuvelliez
Membre du Conseil

Catherine Rutten
Membre du Conseil

Luc Hindryckx
Président du Conseil