Sécurité des réseaux mobiles de 3ème génération

Constantin Yamkoudougou
Ingénieur Réseaux Télécoms & Sécurité, projet PICSI
Laboratoire XLIM UMR CNRS 6172 - Limoges

28 janvier 2005

UMTS ou 3G, quels sont les services attendus ? Quelle sécurité ?

Abstract : the purpose of this document is to getting the reader informed of third generation mobile's new services and also discuss security issues

1 Généralité sur les services UMTS

Les réseaux mobiles UMTS (Universal Mobile Telecommunications System) sont censés apporter plus de confort à l'utilisateur. L'UMTS permet surtout une véritable mobilité multimédia par rapport au WIFI qui n'intègre pas cet aspect lorsqu'il s'agit de passer d'une borne à une autre. Parmi les services les plus en vue, on peut citer le streaming, la messagerie, la visiophonie, les services d'information itinérants.

Le streaming
Le débit nominal des communications en réception est d'environ 380 kbits/s, ce qui permettra un affichage vidéo de bonne qualité sur des terminaux de type PDA de plus de 65000 couleurs et une résoltion de 640x480 pixels ou sur des ordinateurs potables.

Messagerie
Au niveau de la messagerie, l'UMTS permet l'envoi et la réception de MMS vidéo en plus de messages multimédia texte, son et image. Par exemple le GPRS [reférence fiche GPRS-initiation] permet une transmission de photo en moyenne au bout d'une minute. En UMTS quelques secondes suffiront pour transmettre une vidéo.

Visiophonie
Il sera désormais possible d'être vu et de voir directement son interlocuteur sur l'écran du mobile lors d'un appel. Il sera donc possible de partager des événements (partager un lieu, faire voir ce que l'on voit) avec d'autres

personnes, ce qui pouvait se faire difficilement par le téléphone vocal compte tenu des débits de transmission.

Services d'information

Les informations géo-localisées sont les informations qui varient selon la position de l'utilisateur. Selon son déplacement, celui-ci pourra recevoir des informations telles que la météo locale, des informations sur les magasins les plus proches etc.

2 Architecture des réseaux de troisième génération

L'architecture physique d'un réseaux UMTS comporte plusieurs types d'équipements. Le terminal de l'utilisateur, le réseau d'accès connu sous le nom d'UTRAN (UMTS Terrestrian Radio Access Network), les éléments de coeur de réseau que sont le SGSN (Serving GPRS Support Node) et GGSN (Getway GPRS Support Node).

3 Rappel de la sécurité des réseaux de 2ème génération

3.1 Authentification

Deux entités essentielles interviennent dans le mécanisme d'authentification des clients des réseaux de type GSM. Il s'agit d'une part de la carte SIM du terminal d'abonné et d'autre part du centre d'authentification du réseau. Le centre d'authentification et la carte SIM partage une clé sécrète Ki qui n'est jamais transmise sur le réseau. Pour authentifier l'utilisateur, le réseau génère un nombre aléatoire qu'il transmet au mobile et attend une réponse. Le mobile utilise alors une fonction à sens unique appelée fonction A3 qui lui permet de calculer une réponse en utilisant comme paramètres d'entrée la clé secrète Ki et le nombre aléatoire qui lui a été transmis. Ce résultat est ensuite retransmis du terminal mobile vers le centre d'authentification. Le centre d'authentification (AuC) qui connaît également Ki fait le même calcul et le compare au résultat reçu. Si les deux résultats sont identiques, le terminal mobile aura prouvé qu'il connaît le secret partagé Ki et est donc authentifié. Il existe une paire de clé par abonné dans chaque réseau radio-mobile dont l'une est générée dans une puce SIM et l'autre dans la base de donnée d'authentification. Dès lors, on comprend toutes les précautions prises par les opérateurs pour la protection de ces données (controle d'accès, redondance d'architecture, sauvegardes).

3.2 Chiffrement

Dans le cas du chiffrement, le protocole est quasiment le même que celui de l'authentification à l'exception du fait que l'algorithme utilisé pour

la génération de la clé de session est différent. Le nombre pseudo aléatoire qui est généré par le réseau et transmis au mobile est utilisé avec la clé Ki pour générer une clé de session grâce à une fonction nommée A8. La clé de session générée est ensuite utilisée pour chiffrer les trames bit à bit en utilisant l'opérateur XOR. Le centre d'authentification qui sait également calculer la clé de session peut déchiffrer ou chiffrer les trames qu'il reçoit ou émet. Il existe un unique Ki par terminal d'abonné. En pratique le même nombre aléatoire qui a servi lors de l'authentification est simultanément utilisé pour générer la clé de session. Ceci évite l'implémentation d'un protocole spécifique et surtout l'économie de temps et de ressources dans le réseau.

4 Sécurité des réseaux de 2,5 G

La spécificité des réseaux de 2,5 G est la juxtaposition au niveau coeur de réseau d'entités de commutation de paquets distincts des entités classiques de commutation de circuits (MSC) ainsi que des passerelles d'interconnexion avec le réseau public commuté. Dans le système GPRS, l'algorithme de chiffrement utilisé est appelé GEA (GPRS Encryption Algorithm)

5 Sécurité des réseaux de 3ème génération selon les spécifications de 1999

Le standard de la 3 ème génération a évolué de la version initiale datant de 1999 vers les versions plus récentes 4 et 5. La définition des mécanismes de sécurité y a également subi des évolutions pour permettre une migration progressive ou une cohabitation avec des systèmes 2G dont les mécanismes d'authentification et de confidentialité ont déjà été décrits. Les techniques mises en oeuvre pour l'authentification sont beaucoup plus complexes dans les systèmes 3G et intègrent par exemple des mécanismes spécifiques de protection contre le rejeu. La sécurité du protocole de signalisation (MAP) est remise en jeu, ce qui a nécessité la definition de nouvelles spécifications connues sous le nom de MAPSec par le groupe 3GPP. MAPSec s'inspire des mécanismes standard d'IPsec qui est intégrée à la dernière mouture (version 5) des système 3G pour assurer la confidentialité des communications notamment dans les échanges inter opérateurs. L'innovation majeure dans les systèmes de troisième génération est la mise en oeuvre de l'authentification mutuelle.

5.1 Authentification mutuelle.

Le principe de l'authentification mutuelle est une des innovations majeures des systèmes de troisième génération par rapport au systèmes 2G. Dans les systèmes GSM seul le mobile est authentifié par le réseau. Dans les réseaux 3G, trois entités de base sont prises en compte dans le processus d'authentification. Le mobile, le réseau d'accès et le réseau nominal d'origine de l'abonné. Le réseau d'accès est banalisé il peut s'agir d'un réseau mobile visité appartenant à un autre opérateur. La première phase d'authentification est similaire à celle des système 2G à l'exception des algorithmes (lien fiches algorithmes)de dérivation de clés. Elle se fait par challenge / response La seconde phase de l'authentification consiste pour le mobile à s'assurer que le réseau d'accès courant à été légitimé par le réseau coeur d'origine du mobile.

5.1.1 Première phase du processus d'authentification.

Contrairement aux réseaux de 2ème génération pour lesquels l'authentification fait intervenir uniquement le centre d'authentification et le terminal mobile, les organes de localisation type VLR/SGSN jouent un rôle important dans la phase d'authentification. Dès que le VLR/SGSN du réseau visité a connaissance du numéro IMSI (ou TMSI) du terminal mobile, la première étape du processus d'authentification consiste à transmettre ce numéro au centre d'authentification du réseau d'appartenance du mobile. Le centre d'authentification génère un vecteur [hyperlien à développer] à partir de la clé qu'il partage avec la puce USIM du terminal ainsi que deux autres paramètres qui sont : un numéro de séquence et un nombre pseudo aléatoire. Le vecteur d'authentification généré comporte quatre parties : un résultat qui sera demandé dans le challenge/response avec le terminal (XRES), un nombre (AUTN), une clé de session (CK) et une clé de contrôle d'intégrité qui servira à vérifier l'intégrité des messages MACs. Une représentation du protocole peut être vue comme suit.

5.1.2 Deuxième phase du processus d'authentification.

Le VLR /SGSN à la réception du quadruplet (RAND, AUTN, XRES, CK), transmet le challenge RAND et le nombre AUTN qu'il a reçu du VLR/SGSN et attend une réponse RES du mobile. Le protocole de challenge response peut être représenté comme suit :
Le mobile est authentifié si le resultat RES transmis est identique à XRES reçu du centre d'authentification. Le nombre AUTN permet à la puce USIM de vérifier si le centre d'authentification est authentique et qu'il ne s'agit

pas d'une attaque de type man in the middle par le réseau d'accès.

6 Sécurité dans la version 4 et 5 des spécifications de réseaux de troisième génération

Les réseaux informatiques (type TCP/IP) sont structurés en un seul plan avec des protocoles spécifiques pour la supervision et les divers services. Les réseaux de télécommunication sont caractérisés par plusieurs plans : un plan de supervision qui permet de configurer et de maintenir les équipements, un plan de communication qui transmets la parole ou d'autres données d'usagers et le plan de signalistion qui permet de gérér les communications (allocation de canal, fin de communication, etc). Cette signalisation est passée de type voie par voie dans les réseaux analogiques vers une signalisation dite sémaphore plus rapide et performante. A titre d'exemple, pour gerer la signalisation de quelques milliers de canaux de communication un canal de 64 kits est suffisant. Dans le réseaux telephonque fixe d'aujourd'hui, y compris les systèmes mobiles de deuxième et troisième génération, la signalisation est spécifiée au niveau de L'ITU (International Telecommunication Union) par le standard SS7 (Signalling System number 7). Les échanges entre opérateurs reposent sur ce protocole. A titre d'exemple, lorsqu'un abonné se déplace d'un réseaux A vers un réseau B, certains paramètres tels que son identifiant international (IMSI) sont transmis de son réseau d'origine vers le réseau d'arrivée. Dans le protocole SS7, la partie dédiée à la spécification des signalisations dans les réseaux mobiles est le MAP (Mobile Application Part). Lorsqu'il n'y avait qu'un faible nombre de réseaux par pays et que le protocole SS7 n'était connu que par un un nombre restreint de spécialistes, la question de sa sécurité nétait pas encore prépondérante. Aujourd'hui, avec l'explosion des réseaux (densité d'opérateurs par pays) et l'ouverture à des transmissions de type TCP/IP des standards de 3ème génération, sécuriser les échanges inter et même intra réseaux devient primordial. Le protocole MAPsec est la première tentative de spécification de la sécurisation des échanges MAP au sein du groupe 3GPP avant l'intégration du standard IPsec..

7 Sécurisation des échanges entre opérateurs par le protocole MAPSec

Le protocole MAPSec repose sur des mécanismes largement inspirées des associations de sécurité IPSec. Les messages MAP sont chiffrés et encapsulés dans d'autres messages. Un calcul de MAC (Message Authentication

Code) est aussi joint au message MAP chiffré. Le calcul des MAC nécessite l'usage de la cryptographie à clé secrète. Pour résoudre la problématique de la distribution des clés, les clés sont échangées par le biais du protocole de Diffie-Hellman. La gestion des clés se fait par des passerelles de réseau appelées KAC (Key Administration Centre).

8 Quelques références complémentaires

http ://charlotte.ucsd.edu/users/mihir/papers/cbc.html
http ://charlotte.ucsd.edu/users/mihir/papers/sym-enc.html
http ://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html
http ://www.3gpp.org/
http ://www.3gpp.org/ftp/Specs/
http ://www.faqs.org/rfc/rfc3481.txt
http ://www.umtsworld.com/technology/security.htm‘
http ://www.c7.com/ss7/whitepapers/cellular/umts_security.pdf
http ://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/
http ://www.mobilein.com/Training/Update/Update_UMTSSecurity_Concise.htm
UMTS security Valtteri Niemi and Kaisa Nyberg Edition Wiley