On the Security of 3GPP Networks

Michael Walker

Vodafone Airtouch and Royal Holloway College, University of London

(Extended Abstract)

Later this year we shall see the release of the Third Generation Partnership Project (3GPP) specifications for WCDMA – the first third generation standard for mobile communications. This 3G system combines elements of both a radical departure and a timid evolution from the 2G system known as GSM. It is radically different from GSM in having a wide-band CDMA system for its air-interface, but it hangs on to the GSM/GPRS core switching network with its MAP based signalling system. In this paper we consider the security features in WCDMA, taking a critical look at where they depart from those in GSM, where they are still very much the same and how they may develop as the core switching network is replaced by an IP based infrastructure.

Three principles underpinned the approach adopted for security in WCDMA: build on 2G by retaining security features from GSM that have proved to be needed and robust; address the weaknesses in 2G, both the real and the perceived ones; introduce new features where new 3G architectures and services demand them. In addition there was the desire to retain as much compatibility with GSM as possible in recognition of the fact that many WCDMA networks would be rolled out alongside GSM networks, with them sharing a core switching network, and with handover of calls between the two.

The problems with GSM security derive not so much from intrinsic problems with the mechanisms (although we will consider the algorithms separately) but rather from deliberate restrictions on the design. The most significant restriction was that GSM only needed to be as secure as the fixed networks. This was interpreted to mean that wherever fixed network technology was used cryptographic features were not needed. After all, they were not, and still are not, used by fixed carriers to protect consumer services. Fixed links in a mobile network were excluded from consideration, as was mobile signalling data when transferred over fixed networks. Protection against attacks involving impersonating a network element was not addressed. All this has led to three real security concerns for GSM: the use of false base stations to intercept mobile originated calls, interception of microwave links between base stations and the core network, and the vulnerability of signalling to interception and impersonation. We will consider each of these concerns and explain how they have been addressed in WCDMA.

The GSM algorithms were designed at a time when the political climate was very different from what it is today. It was radical to launch a public access

telecommunications system that automatically provided encryption – open evaluation and publication of the algorithm design criteria was just not an option. But the system was designed so that operators could use the best authentication algorithms available – so why was one used that is so obviously flawed? We look at these problems, and the rather different approach taken for the WCDMA algorithms.

All these considerations have led to the following set of security features in the first release of the WCDMA standard. Encryption of user traffic and signalling data on the air-interface, with the encryption terminated in the network at the RNC (radio network controller). This is further into the network than with GSM, where termination is at the base station. In addition to encryption, there is an integrity check on the air-interface signalling data. Authentication uses the same challenge-response technique as in GSM, except that it is enhanced to allow the mobile to verify the origin and freshness of the challenge. The basic key management is unchanged from GSM. The SIM still features as the security processor in the mobile terminal, and it shares an authentication key with its home network. This key is used to generate authentication data and encryption and integrity keys used to protect traffic in the access network. The security protocol is still executed in the local access network, but the network signalling is now protected. Thus user authentication data and ciphering keys can be encrypted when they are transferred between or within networks on signalling links.

The cryptographic keys for encryption and integrity are longer than those used in GSM, and a more open approach has been adopted for the design and evaluation of the air-interface algorithm. At the time of writing the algorithm has not been published, but it is hoped that it will be available on the ETSI web site shortly. As we shall see, the algorithm is very different from that used in GSM.

So for the first release of the WCDMA standards, the so-called release 99 or R99, the security features are more-or-less an upgraded version of those used in GSM. In particular, we still have a set of security features for an access network. This was to be expected, since the focus to date of 3GPP standardisation has been to define WCDMA as a new radio access to the GSM/GPRS switching network. The emphasis for R00 is now shifting to an IP based core network. We shall see that this is resulting in a set of additional security features.