WHITE PAPER

CDMA 1XRTT SECURITY OVERVIEW

August, 2002

Contacts:

Christopher Wingert

Mullaguru Naidu

T A B L E O F C O N T E N T S

1. Executive Summary

Since the birth of the cellular industry, security has been a major concern for both service providers and subscribers. Service providers are primarily concerned with security to prevent fraudulent operations such as cloning or subscription fraud, while subscribers are mainly concerned with privacy issues. In 1996, fraudulent activities through cloning and other means cost operators some US$750 million in lost revenues in the United States alone. Fraud is still a problem today, and IDC estimates that in 2000, operators lost more than US$180M in revenues from fraud. Technical fraud, such as cloning, is decreasing in the United States, while subscription fraud is on the rise[1]. In this paper, we will limit our discussions to technical fraud only. With the advent of second-generation digital technology platforms like TDMA/CDMA-IS-41, operators were able to enhance their network security by using improved encryption algorithms and other means. The noise-like signature of a CDMA signal over the air interface makes eavesdropping very difficult. This is due to the CDMA "Long Code," a 42-bit PN (Pseudo-Random Noise of length 2^{42}-1) sequence, which is used to scramble voice and data transmissions.

This paper discusses how CDMA 2000 1xRTT implements three major features of mobile security: authentication, data protection, and anonymity.

2. *Security – CDMA Networks*

The security protocols with CDMA-IS-41 networks are among the best in the industry. By design, CDMA technology makes eavesdropping very difficult, whether intentional or accidental. Unique to CDMA systems, is the 42-bit PN (Pseudo-Random Noise) Sequence called "Long Code" to scramble voice and data. On the forward link (network to mobile), data is scrambled at a rate of 19.2 Kilo symbols per second (Ksps) and on the reverse link, data is scrambled at a rate of 1.2288 Mega chips per second (Mcps).

CDMA network security protocols rely on a 64-bit authentication key (A-Key) and the Electronic Serial Number (ESN) of the mobile. A random binary number called RANDSSD, which is generated in the HLR/AC, also plays a role in the authentication procedures. The A-Key is programmed into the mobile and is stored in the Authentication Center (AC) of the network. In addition to authentication, the A-Key is used to generate the sub-keys for voice privacy and message encryption.

CDMA uses the standardized CAVE (Cellular Authentication and Voice Encryption) algorithm to generate a 128-bit sub-key called the "Shared Secret Data" (SSD). The A-Key, the ESN and the network-supplied RANDSSD are the inputs to the CAVE that generates SSD. The SSD has two parts: SSD_A (64 bit), for creating authentication signatures and SSD_B (64 bit), for generating keys to encrypt voice and signaling messages. The SSD can be shared with roaming service providers to allow local authentication. A fresh SSD can be generated when a mobile returns to the home network or roams to a different system.

2.1. Authentication

In CDMA networks, the mobile uses the SSD_A and the broadcast RAND* as inputs to the CAVE algorithm to generate an 18-bit authentication signature (AUTH_SIGNATURE), and sends it to the base station. This signature is then used by the base station to verify that the subscriber is legitimate. Both Global Challenge (where all mobiles are challenged with same random number) and Unique Challenge (where a specific RAND is used for each requesting mobile) procedures are available to the operators for authentication. The Global Challenge method allows very rapid authentication. Also, both the mobile and the network track the Call History Count (a 6-bit counter). This provides a way to detect cloning, as the operator gets alerted if there is a mismatch.

* Broadcast RAND, generated in the MSC, should not be confused with the RANDSSD from the HLR*

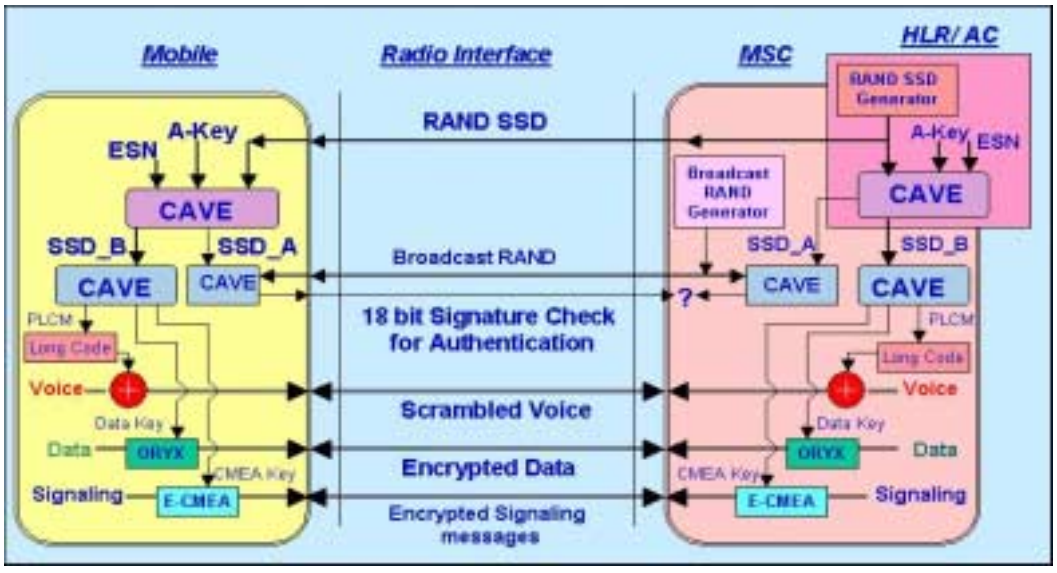
The A-Key is re-programmable, but both the mobile and the network Authentication Center must be updated. A-Keys may be programmed by one of the following: a) The factory b). The dealer at the point of sale c) Subscribers via telephone d) OTASP (over the air service provisioning). OTASP transactions utilize a 512-bit Diffie-Hellman key agreement algorithm, making them well suited for this function. The A-Key in the mobile can be changed via OTASP, providing an easy way to quickly cut off service to a cloned mobile or initiate new services to a legitimate subscriber. Security of the A-Key is the most important component of CDMA system.

2.2. Voice, Signaling, and Data Privacy

The mobile uses the SSD_B and the CAVE algorithm to generate a Private Long Code Mask (derived from an intermediate value called Voice Privacy Mask, which was used in legacy TDMA systems), a Cellular Message Encryption Algorithm (CMEA) key (64 bits), and a Data Key (32 bits). The Private Long Code Mask is utilized in both the mobile and the network to change the characteristics of a Long code. This modified Long code is used for voice scrambling, which adds an extra level of privacy over the CDMA air interface. The Private Long Code Mask doesn't encrypt information, it simply replaces the well-known value used in the encoding of a CDMA signal with a private value known only to both the mobile and the network. It is therefore extremely difficult to eavesdrop on conversations without knowing the Private Long Code Mask.

Additionally, the mobile and the network use the CMEA key with the Enhanced CMEA (E-CMEA) algorithm to encrypt signaling messages sent over the air and to decrypt the information received. A separate data key, and an encryption algorithm called ORYX, are used by the mobile and the network to encrypt and decrypt data traffic on the CDMA channels. Figure 3 illustrates the CDMA authentication and encryption mechanism.

FIGURE 3:



By design, all CDMA phones use a unique PN (Pseudo-random Noise) code for spreading the signal, which makes it difficult for the signal to be intercepted.

2.3. Anonymity

CDMA systems support the assignment of a Temporary Mobile Station Identifier (TMSI) to a mobile to represent communications to and from a certain mobile in over the air transmissions. This feature makes it more difficult to correlate a mobile user's transmission to a mobile user.

3. 3g CDMA 2000 Security

Third Generation technologies add more security protocols, including the use of 128-bit privacy and authentication keys. For CDMA2000 networks, new algorithms such as Secure Hashing Algorithm-1 (SHA-1) are being used for hashing and integrity, and the Advanced Encryption Standard, AES (Rijndael) algorithm for message encryption. The AKA (Authentication and Key Agreement) protocol will be used for all releases following CDMA2000 Release C. The AKA protocol will also be used in WCDMA-MAP networks, along with the Kasumi algorithm for encryption and message integrity.

References

1. Authentication and Security in Mobile Phones by Greg Rose, Qualcomm Inc., Australia.
2. Security in CDMA Wireless Systems by Frank Quick, Qualcomm Inc., February 1997
3. Security Aspects of Mobile Wireless Networks, by Mullaguru Naidu, July 2002.

Appendix: Glossary

AC (AuC)	Authentication Center
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
CAVE	Cellular Authentication and Voice Encryption
CDMA	Code Division Multiple Access
CMEA	Cellular Message Encryption Algorithm
ESN	Electronic Serial Number
HLR	Home Location Register
IDC	International Data Corporation
IS	Interim Standard
MAP	Mobile Applications Part
MSC	Mobile Switching Center
OTASP	Over The Air Service Provisioning
RAND	RANDom challenge
SHA-1	Secure Hash Algorithm -1
SSD	Shared Secret Data
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Station Identifier