Chapter 1
Debilities of the UMTS Security Mode Set-Up Procedure and Attacks against UMTS/HSPA Device

Diego Fernández Alonso
University of Vigo, Spain

Ana Vázquez Alejos
University of Vigo, Spain

Manuel García Sánchez
University of Vigo, Spain

ABSTRACT

A study and identification of vulnerabilities during the set-up procedure of the Universal Mobile Telecommunication System (UMTS) and how some of them can be exploited. For accomplishment a good understanding of the security messages exchange, a part of UMTS architecture is developed firstly. After the explanation of the security mode set-up procedure debilities, the chapter identify attacks that take advantage of the fact that some messages during their exchange in the process are not protected. The attacks indicated in the chapter are mostly of Denial of Service (DoS) kind, and mainly are performed with a rogue BTS.

DOI: 10.4018/978-1-4666-8687-8.ch001

INTRODUCTION

The UMTS is the acronym of Universal Mobile Telecommunication System developed by the 3rd Generation Partnership Project (3GPP). The UMTS standard is based on WCDMA (Wideband Code Division Multiple Access) for the radio interface (Uu). This interface uses CDMA (Code Division Multiple Access) as access method and can operate in two ways, FDD (Frequency Division Duplex) and TDD (Time Division Duplex).

Nowadays HSPA (High Speed Packet Access) is used for the Up Link (HSUPA) and the Down Link (HSDPA). HSPA is an upgrade of WCDMA and was introduced by parts. The HSDPA (High Speed Down Link Packet data Access) was introduced in 3GPP Release 5 and the HSUPA (High Speed Up Link Packet data Access) was introduced in 3GPP Release 6. HSPA is the combination of both.

HSPA represents the 3rd generation of mobile communication technology and provides mutual authentication, confidentiality and integrity.

One of the part of UMTS architecture more vulnerable is the network access, since is where there are the mainly threats. The mainly vulnerabilities over UMTS are in relation with the security mode set-up and transmission of keys and data in text clear in its process. The Authentication and Key Agreement (AKA) and encryption and integrity algorithms are very robust, the vulnerabilities exist due the way the system have for start the security establishment with those algorithms.

To take advantage of the UMTS vulnerabilities is not easy due it is necessary to have knowledge about specific resources, like the software to configure a Base Transceiver Station (BTS). Although there are vulnerabilities through the complete architecture, for an intruder the easier interface to perform the attacks is the radio interface or Uu (in UMTS).

UMTS ARCHITECTURE

The architecture of Universal Mobile Telecommunications System (UMTS) includes three different domains, UMTS Terrestrial Radio Access Network (UTRAN), Core Network (CN) and User Equipment (UE).

The UTRAN provides the air interface access method for the User Equipment through the Base Station (BS) or Node-B. Core Network provides switching, routing and transit for the user traffic, and it contains the databases and network management functions. And finally User Equipment is the terminal that allows the mobile communication of the user through the air interface.