Chapter XXI
Access Security in UMTS and IMS

Yan Zhang
Simula Research Laboratory, Norway

Yifan Chen
University of Greenwich, UK

Rong Yu
South China University of Technology, China

Supeng Leng
University of Electronic Science and Technology of China, China

Huansheng Ning
Beihang University, China

Tao Jiang
Huazhong University of Science and Technology, China

INTRODUCTION

Motivated by the requirements for higher data rate, richer multimedia services, and broader radio range wireless mobile networks are currently in the stage evolving from the second-generation (2G), for example, global system for mobile communications (GSM), into the era of third-generation (3G) or beyond 3G or fourth-generation (4G). Universal mobile telecommunications system (UMTS) is the natural successor of the current popular GSM (http://www.3gpp.org) code division multiple access 2000 (CDMA2000) is the next generation version for the CDMA-95, which is predominantly deployed in North America and North Korea. Time division-sychrononous CDMA (TD-SCDMA) is in the framework of 3rd generation partnership project 2 (3GPP2) and is expected to be one of the principle wireless technologies employed in China in the future (http://www.3gpp.org; 3G TS 35.206). It is envisioned that each of three standards in the framework of international mobile telecommunications-2000 (IMT-2000) will play a significant role in the future due to the backward compatibility, investment, maintenance cost, and even politics. In all of the potential standards, access security is one of the primary demands as well as challenges

to resolve the deficiency existing in the second generation wireless mobile networks such as GSM, in which only one-way authentication is performed for the core network part to verify the user equipment (UE) (3G TS 24.008). Such access security may lead to the "man-in-middle" problem, which is a type of attack that can take place when two clients are communicating remotely and exchange public keys in order to initialize secure communications. If both of the two public keys are intercepted in the route by someone, he/she can act as a conduit and send in the messages with his/her own faked public key. As a result, the secure communication is eavesdropped by a third party.

Multimedia service provisioning is one of the primary demands and motivations for the next generation wireless networks. To achieve this goal, the IP multimedia subsystem (IMS) is added as the core network in UMTS providing the multimedia service, for example, voice telephony, video conference, real-time streaming media, interactive game, voice over IP, picture, HTTP, and instant messaging (3G TS 33.203). The multimedia session management, initialization, and termination are specified and implemented in the session initiation protocol (SIP) (3G TS 29.228; Zhang & Fang, 2005). To ensure the secure communication in a multimedia session, an efficient access security mechanism shall be also provided.

In this chapter, we make an introduction to the access security in the next generation wireless mobile networks, including the mechanisms in the circuited-switched domain, packet-switched domain, and also the emerging IMS domain.

BACKGROUND OVERVIEW

Figure 1 shows the UMTS network architecture with most related components in security management (3G TS 29.002; 3G TS 33.102). User terminal (UE) utilizes the circuited-switched or packet-switched service through the radio interface between base station (BS) and itself. BS locates in the center of a cell which coveres a radio range. BS provides the wireless access point for UEs to the core network. Radio network controller (RNC) monitors and supervises the activities of several BS under its management. Radio access network (RAN) consists of the RNC and the associated BS under the RNC. Home location register (HLR) stores the permanent information for the subscrib-

Figure 1. UMTS network architecture