Chapter XXII
Security in 2.5G Mobile Systems

Christos Xenakis
University of Piraeus, Greece

ABSTRACT

The global system for mobile communications (GSM) is the most popular standard that implements second generation (2G) cellular systems. 2G systems combined with general packet radio services (GPRS) are often described as 2.5G, that is, a technology between the 2G and third generation (3G) of mobile systems. GPRS is a service that provides packet radio access for GSM users. This chapter presents the security architecture employed in 2.5G mobile systems focusing on GPRS. More specifically, the security measures applied to protect the mobile users, the radio access network, the fixed part of the network, and the related data of GPRS are presented and analyzed in detail. This analysis reveals the security weaknesses of the applied measures that may lead to the realization of security attacks by adversaries. These attacks threaten network operation and data transfer through it, compromising end users and network security. To defeat the identified risks, current research activities on the GPRS security propose a set of security improvements to the existing GPRS security architecture.

INTRODUCTION

The global system for mobile communications, (GSM) is the most popular standard that implements second generation (2G) cellular systems. 2G systems combined with general packet radio services (GPRS) (3GPP TS 03.6, 2002) are often described as 2.5G, that is, a technology between the 2G and third generation (3G) of mobile systems. GPRS is a service that provides packet radio access for GSM users. The GPRS network architecture, which constitutes a migration step toward 3G systems, consists of an overlay network onto the GSM network. In the wireless part, the GPRS technology reserves radio resources only when there is data to be sent, thus, ensuring the optimized utilization of radio resources. The fixed part of the network employs the IP technology and is connected to the public Internet. Taking advantage of these features, GPRS enables the provision of a variety of packet-oriented multimedia applications and services to mobile users, realizing the concept of the mobile Internet.

For the successful implementation of the new emerging applications and services over GPRS, security is considered as a vital factor. This is because of the fact that wireless access is inherently less secure and the radio transmission is by nature more susceptible to eavesdropping and fraud in use than wire-line transmission. In addition, users' mobility and the universal access to the network imply higher security risks compared to those encountered in fixed networks. In order to meet security objectives, GPRS uses a specific security architecture, which aims at protecting the network against unauthorized access and the privacy of users. This architecture is mainly based on the security measures applied in GSM, since the GPRS system is built on the GSM infrastructure.

Based on the aforementioned consideration, the majority of the existing literature on security in 2.5G systems refers to GSM (Mitchell, 2001; Pagliusi, 2002). However, GPRS differs from GSM in certain operational and service points, which require a different security analysis. This is because GPRS is based on IP, which is an open and wide deployed technology that presents many vulnerable points. Similarly to IP networks, intruders to the GPRS system may attempt to breach the confidentiality, integrity, or availability, or otherwise attempt to abuse the system in order to compromise services, defraud users, or any part of it. Thus, the GPRS system is more exposed to intruders compared to GSM.

This chapter presents the security architecture employed in 2.5G mobile systems focusing on GPRS. More specifically, the security measures applied to protect the mobile users, the radio access network, the fixed part of the network, and the related data of GPRS are presented and analyzed in details. This analysis reveals the security weaknesses of the applied measures that may lead to the realization of security attacks by adversaries. These attacks threaten network operation and data transfer through it, compromising end users and network security. To defeat the identified risks, current research activities on the GPRS security propose a set of security improvements to the existing GPRS security architecture. The rest of this chapter is organized as follows. The next section describes briefly the GPRS network architecture. The third section presents the security architecture applied to GPRS and the fourth section analyzes its security weaknesses. The fifth section elaborates on the current research activities on the GPRS security and the sixth section presents the conclusions.

GPRS NETWORK ARCHITECTURE

The network architecture of GPRS (3GPP TS 03.6, 2002) is presented in Figure 1. A GPRS user owns a mobile station (MS) that provides access to the wireless network. From the network side, the base station subsystem (BSS) is a network part that is responsible for the control of the radio path. BSS consists of two types of nodes: the base station controller (BSC) and the base transceiver station (BTS). BTS is responsible for the radio coverage of a given geographical area, while BSC maintains radio connections towards MSs and terrestrial connections towards the fixed part of the network (core network).

The GPRS core network (CN) uses the network elements of GSM such as the home location register (HLR), the visitor location register (VLR), the authentication centre (AuC) and the equipment identity register (EIR). HLR is a database used for the management of permanent data of mobile users. VLR is a database of the service area visited by an MS and contains all the related information required for the MS service handling. AuC maintains security information related to subscribers identity, while EIR maintains information related to mobile equipments' identity. Finally, the mobile service switching centre (MSC) is a network element responsible for circuit-switched services (e.g., voice call) (3GPP TS 03.6, 2002).

As presented previously, GPRS reuses the majority of the GSM network infrastructure. However, in order to build a packet-oriented mobile network some new network elements (nodes) are required, which handle packet-based traffic. The new class of nodes, called GPRS support nodes (GSN), is responsible for the delivery and routing of data packets between an MS and an external packet data network (PDN). More specifically, a serving