Vulnerabilities and Possible Attacks Against the GPRS Backbone Network

Christos Xenakis and Lazaros Merakos

Security Group, Communication Networks Laboratory
Department of Informatics & Telecommunications, University of Athens
15784 Athens, Greece
{xenakis,merakos}@di.uoa.gr
http://www.cnl.di.uoa.gr/

Abstract. This paper presents the security weaknesses and the possible attacks, which threaten the GPRS backbone network and the data that either reside at the network or are transferred through it. These attacks may be performed by malicious third parties, mobile users, network operators or network operator personnel, which exploit the weaknesses of the employed technology and the security measures applied to the GPRS backbone. The possible attacks against the GPRS backbone may result in the compromise of end-users security, the users over billing, the disclosure or alteration of critical information, the services unavailability, the network breakdown, etc. The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept of the mobile Internet.

1 Introduction

The General Packet Radio Services (GPRS) [1] is a service that provides packet radio access for Global System for Mobile Communications (GSM) users. The GPRS network architecture, which constitutes a migration step toward third-generation (3G) communication 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. 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 based on the security measures applied in GSM, since the GPRS system is built on the GSM infrastructure. However, GPRS is more exposed to intruders compared to GSM [2][3]

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 262 – 272, 2006.

because it uses the IP technology, which presents known vulnerabilities. Similarly to IP networks, intruders to the GPRS system may attempt to breach the confidentiality, integrity, availability or otherwise attempt to abuse the system in order to compromise services, defraud users or any part of it.

This paper presents the security weaknesses and the possible attacks, which threaten the GPRS backbone network and the data that either reside at the network or are transferred through it. These attacks may be performed by malicious third parties, mobile users, network operators or network operator personnel, which exploit the weaknesses of the employed technology and the security measures applied to the GPRS backbone. The possible attacks against the GPRS backbone may result in the compromise of end-users security, the users over billing, the disclosure or alteration of critical information, the services unavailability, the network breakdown, etc. The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept of the mobile Internet.

The rest of this article is organized as follows. Section 2 briefly describes the GPRS technology and the security measures applied to the GPRS backbone network. Section 3 presents the weaknesses of the security measures applied to the GPRS backbone. Section 4 analyzes the possible attacks that threaten the GPRS backbone and the data that either reside at the network or are transferred through it. Finally, section 5 contains the conclusions.

2 GPRS Technology

2.1 Network Architecture

The network architecture of GPRS [1] is presented in Fig.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) [1].