EFFICIENT AUTHENTICATION AND KEY AGREEMENT PROCEDURE IN IP MULTIMEDIA SUBSYSTEM FOR UMTS

Hung-Min Sun, Bing-Zhe He, Shih-Ying Chang and Chun-Hua Cho

Department of Computer Science
National Tsing Hua University
No. 101, Sec. 2, Kuang-Fu Road, Hsinchu 30013, Taiwan
hmsun@cs.nthu.edu.tw

Received November 2010; revised May 2011

ABSTRACT. In a Universal Mobile Telecommunications System (UMTS), a user equipment (UE) can access IP multimedia services through IP Multimedia Subsystems (IMS). In addition to passing IMS authentication, called IMS AKA, this UE also needs to pass General Packet Radio Service (GPRS) authentication, called 3GPP AKA, since the data of the IMS service is transmitted through a GPRS network. Many steps in these two authentication processes are identical and result in inefficiency. Two papers proposed efficient authentication schemes instead of IMS authentication. However, these schemes suffer from security and compatibility problems. In this paper, we design an efficient IMS authentication scheme based on a trust relation between UE and Serving GPRS Support Node (SGSN) established in GPRS authentication. Compared with the conventional IMS authentication, our scheme can save up to 40% transmission and is analyzed as a secure scheme. Moreover, our scheme does not require any modification in the UE’s authentication procedures.

Keywords: 3GPP AKA, IMS AKA, Authentication

1. Introduction. To provide different types of services for a user, integration of different heterogeneous wireless network environments is a rising and important issue in recent years. Future telecommunication networks will converge on an All-IP network; that is, users will be able to access data from one or more different wireless network interfaces. Universal Mobile Telecommunications System (UMTS) proposed by the Third-Generation Partnership Project (3GPP) is a third-generation (3G) mobile communication technology. UMTS supports IP-based multimedia services, such as audio, video, text and chat, through IP Multimedia Subsystem (IMS) [1]. Many recent studies have investigated authentication and key agreement for protecting the communications [16-19]. A user can easily establish a session key for encryption and authentication. The authentication mechanism for 3G is called AKA and defined in RFC3310, which is used in GPRS network and IMS.

The UMTS architecture is illustrated in Figure 1. UE accesses the services by Serving GPRS Support Node (SGSN) through UMTS terrestrial radio access network (UTRAN). The SGSN connects to the home subscriber server (HSS) and the authentication center (AuC) to obtain authentication information. In addition, SGSN connects to Call Session Control Functions (CSCFs) and data network via gateway GPRS support node (GGSN) in order to support IP multimedia services and so on.

In UMTS, user equipment (UE) can access services, GPRS services and IMS services. If a UE wants to access GPRS services, the UE and the SGSN must authenticate with each other via GPRS authentication [2]. If the UE wants to use IMS services, besides the GPRS authentication, the UE has to be authenticated by the IMS authentication [3].