Undeniable Mobile Billing Schemes*

Shiqun Li[1,2], Guilin Wang[2], Jianying Zhou[2], and Kefei Chen[1]

[1] Dep. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China
[2] Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613

Abstract. An undeniable mobile billing system allows a mobile network service provider to bill its subscribers with trustworthy evidences. Chen, Jan and Chen proposed such a billing system by introducing a trusted third party – Observer and exploiting a hash chain mechanism. In their system, the Observer provides call time evidence to both cellular carriers and subscribers for billing. In this paper, we first identify some vulnerabilities in their mobile billing system. Then, we propose an undeniable billing scheme based on a proper combination of digital signature and hash chain mechanism. The proposed scheme can achieve authentication, non-repudiation, and fairness, which are desirable security requirements for an undeniable mobile billing system.

1 Introduction

In the traditional GSM billing system, both the billing management and the billing information are processed by the Mobile Network Service Provider (MNSP) alone. From the subscribers' point of view, the above method may be not a good solution. Therefore, Chen et al. [3] proposed a mobile billing scheme (CJC scheme, for short) to provide undeniable billing evidences for call services in GSM. They introduced a TTP – Observer and used hash chain to provide billing information. The Observer is in charge of authentication and evidence provision.

In this paper, we first identify some vulnerabilities in the CJC system. Then we propose a new undeniable billing scheme, which is based on a proper combination of digital signature and a hash chain mechanism. It is very lightweight and suitable for the GSM mobile phone users.

The rest of the paper is organized as follows. Section 2 briefly introduces existing mobile billing systems. Section 3 reviews the CJC scheme and analyzes its security. Section 4 presents the proposed mobile billing systems which is based on hash chain technique and digital signatures. Section 5 evaluates the proposed scheme in aspects of security and efficiency. Section 6 draws a conclusion.

* Project supported by the National Nature Science Foundation of China key project(No.90104005) and Specialized Research Fund for the Doctoral Program of Higher Education(No. 20050248043). The primary author's work was done during his attachment to the Institute for Infocomm Research under its sponsorship.

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 338–345, 2007.

2 Mobile Billing Systems

To provide undeniable evidences for mobile network services, several schemes were proposed. The undeniable billing system in mobile communication [6] proposed an efficient solution to undeniable billing when a mobile user roams into foreign networks. This scheme adopted public key cryptographic algorithm to provide authentication and non-repudiation evidences, which is complicated for the current GSM mobile terminals. The Secure Billing for Mobile Information Services [2,4], provided a secure billing scheme for value-added information services using micropayment mechanism. It also requires public key operations for the mobile terminal which is applicable for UMTS mobile users but not the current GSM mobile users.

The CJC scheme [3] introduced an Observer as the TTP and used hash chain mechanism to provide billing information. It is a very efficient for mobile users, since the MSU is not required to perform any asymmetric cryptographic operation. However, our analysis shows that the CJC mobile billing system has some vulnerabilities so that it is not applicable in practice.

Our main purpose in this paper is to propose a new mobile billing scheme such that it is secure and as efficient as the CJC scheme. That is, we do not require the user's MSU do any public key operation (so our work is different from [2,4,6]). On the other hand, as in [6] we also employ the hash chain technique to determine the duration of a call service.

3 CJC Scheme and Its Vulnerabilities

3.1 Review of the CJC Scheme

The CJC mobile billing system [3] is illustrated in Fig. 1. As shown in Fig. 1, the Observer acts as the agent of a subscriber's MSU and shares a hash chain with it. To generate the bill evidence for a call, the MSU will first be authenticated by the MNSP and the Observer. Then the MNSP and the Observer sign the start time and end time of a valid call. Thus, by exploiting the hash chain technique and digital signature mechanism, both the MNSP and the subscriber cannot forge or deny the valid billing records. Note that here the Observer acts as a TTP and is in charge of providing call evidences to both the mobile subscriber and the MNSP. For more details about the CJC scheme, please refer to [3].

The authors claimed that their system satisfies the requirements of a fair mobile billing system. However, our analysis below will show that the CJC scheme cannot provide practicability and non-repudiation as supposed.

3.2 Vulnerabilities in the CJC Scheme

In this part, we show some vulnerabilities in the CJC mobile billing scheme [3]. Some of them are security flaws, and others are about implementation weaknesses.

First of all, the CJC scheme is *not fair* for both the MNSP and the mobile users. We now show two attacks on the fairness of the CJC scheme.