Chapter 8
On the Security of Self-Certified Public Keys

Cheng-Chi Lee
Fu Jen Catholic University, Taiwan

Min-Shiang Hwang
Asia University, Taiwan

I-En Liao
National Chung Hsing University, Taiwan

ABSTRACT

Many cryptosystems have been developed to solve the problem of information security, and some approaches are based on the self-certified public key proposed by Girault. In Girault’s scheme, the public key is computed cooperatively by both the system authority (SA) and the user. One of the advantages is that the public key is able to implicitly authenticate itself without any additional certificates. Another advantage is that the SA is not able to forge a public key without knowing the user’s secret key. Despite the advantages of Girault’s system, in this paper, the authors demonstrate that the system still suffers from two main weaknesses. As a result, the authors propose a slight improvement on Girault’s system.

INTRODUCTION

Some well-known public key systems have been developed since 1976 (Diffie & Hellman, 1976; ElGamal, 1985; Hwang, Chang, & Hwang, 2002; Rivest, Shamir, & Adleman, 1978). In those systems, each user has two keys, namely, the private key and the public key. The private key is kept secretly by a user, and it is used to provide the legal signature of a message or to decrypt a message sent by another user. The public key is accessible to public through directory lookup, and it is used to verify the validity of a signature or to encrypt a message. Since the public key is published to the public key directory, an adversary can modify the public key of a target user from the public key directory. A public-key authentication is an important research’s issue. The purpose of
public-key authentication is to verify the public key of a legal user and to prevent public key from being forged.

Three of the most popular schemes for public-key authentication are ID-based scheme (Shamir, 1984), certificate-based scheme (Kohnfelder, 1978) and self-certified scheme (Girault, 1991). We briefly review each of them in the following.

In ID-based scheme, a user first chooses his/her own secret key, and then the system authority (SA) generates a public key using the user’s identity and the secret key. Since the public key is derived from the user’s identity, the direct relation between the identity and the public key makes it impossible for an evil user to forge a public key. In addition, there is no need to store the public key in a public directory. However, this scheme has a drawback that the SA can impersonate a user, since SA knows every user’s secret key. In general, public keys are derived from user’s identities and secret keys. For example, the public key is equal to \( s = ID^d \mod n \), where \( ID \) is user’s identity and \( d \) is user’s secret key. This procedure is generated by SA.

In certificate-based scheme, the public key of a user is generated by the SA and is used as the user’s certificate. The process of generating a public key is also known to the public. The difference between ID-based scheme and certificate-based scheme is that the certificate-based scheme has a certificate to verify the public key of a user. The procedure of generating public keys is public. For example, the public is \( (y, C) \), where \( y \) is user’s public key and \( C \) is the public key’s certificate. Therefore, one can recalculate a user’s public key and compare it with the one stored in the SA’s system to verify the validity of a public key. These schemes suffer from the same drawback as in the ID-based scheme, namely, the SA is able to impersonate a user by generating a false certificate. In addition, the certificates have to be stored in SA’s system which may occupy too much storage space.

The self-certified scheme was developed by Girault to overcome the problems of the above two, in which a user first chooses his/her own secret key, and then the public key is computed using both the user’s and SA’s secret keys. That is to say, the public key is generated by both of user and SA. If SA doesn’t know the user’s secret key, SA cannot generate public key. The detail of this procedure can be seen in another section. The main feature of this system is that the SA is a trusted party. The SA is unable to forge a public key. In other words, it makes the SA more trustworthy. Due to such an advantage, this scheme received a lot more attentions than the other schemes did (Chang, Wu, & Huang, 2000; Saeednia, 1997; Saeednia & Ghodosi, 1999; Tseng & Jan, 1999; Yang, Choi, & Ann, 1996). These schemes also need an SA to help users to sign users’ public keys. The public key is computed by using both of the user’s and SA’s secret keys. Therefore, SA cannot impersonate a user to derive a user’s public key. Using the Girault’s system, theses schemes can achieve their proposed requirements.

Despite the advantages of Girault’s system, Saeednia showed that their system is insecure (Saeednia, 2003). Saeednia pointed out that the authority SA can know the users’ secret keys if the authority generates modulo \( n \) in a special dishonest way. In this paper, we will propose a different cryptanalysis of the system. We assume that the authority is a trusted party. This paper will show two weaknesses that an evil user who impersonates the SA and generates a legal public key of a user without knowing the secret key of the SA. Next, we will propose a slight improvement on Girault’s system.

The rest of the paper is organized as follows. In the next section, the Girault’s self-certified public key is briefly reviewed. The problem of Girault’s system is described. Finally, we give a few concluding remarks and a slight improvement.

**GIRAULT’S SELF-CERTIFIED PUBLIC KEY SYSTEM**

Girault proposed a self-certified public key system (Girault, 1991) that is based on the RSA
Related Content

Key Distribution and Management for Mobile Applications
[www.igi-global.com/chapter/key-distribution-management-mobile-applications/22046?camid=4v1a](www.igi-global.com/chapter/key-distribution-management-mobile-applications/22046?camid=4v1a)

Face Recognition Technology: A Biometric Solution to Security Problems
[www.igi-global.com/chapter/face-recognition-technology/23339?camid=4v1a](www.igi-global.com/chapter/face-recognition-technology/23339?camid=4v1a)

Reducing Risk through Segmentation, Permutations, Time and Space Exposure, Inverse States, and Separation

TCP/IP Reassembly in Network Intrusion Detection and Prevention Systems