A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes*

Qiang Tang[1,**], Julien Bringer[2], Hervé Chabanne[2], and David Pointcheval[3]

[1] DIES, EWI, University of Twente, the Netherlands
[2] Sagem Sécurité
[3] Departement d'Informatique, École Normale Supérieure
45 Rue d'Ulm, 75230 Paris Cedex 05, France

Abstract. With their increasing popularity in cryptosystems, biometrics have attracted more and more attention from the information security community. However, how to handle the relevant privacy concerns remains to be troublesome. In this paper, we propose a novel security model to formalize the privacy concerns in biometric-based remote authentication schemes. Our security model covers a number of practical privacy concerns such as identity privacy and transaction anonymity, which have not been formally considered in the literature. In addition, we propose a general biometric-based remote authentication scheme and prove its security in our security model.

1 Introduction

Privacy has become an important issue in many aspects of our daily life, especially in an era of networking where information access may go far beyond our control. When sensitive information such as biometrics is used, the privacy issues become even more important because corruption of such information may be catastrophic for the relevant applications. In this paper we focus on the issue of handling the privacy concerns in remote biometric-based authentication schemes.

1.1 Related Work

Biometrics, such as fingerprint and iris, have been used to a higher level of security in order to cope with the increasing demand for reliable and highly-usable information security systems, because they have many advantages over typical cryptographic credentials. For example, biometrics are believed to be unique, unforgettable, non-transferable, and they do not need to be stored. One of the most important application areas is biometric-based authentication schemes, where an authentication is simply a comparison between a reference biometric template

* This work is partially supported by French ANR RNRT project BACH.

** The work was done when the author worked as a postdoc researcher at École Normale Supérieure.

L. Chen, Y. Mu, and W. Susilo (Eds.): ISPEC 2008, LNCS 4991, pp. 56–70, 2008.

and a new template extracted during the authentication process. Note that, depending on the type of biometrics, comparison may mean image matching, binary string matching, etc.

Despite of its advantages, in practice, there are some obstacles in a wide adoption of biometrics.

First, biometrics are only approximately stable over the time, therefore, they cannot be directly integrated into most of the existing systems. To address this issue, error-correction concept is widely used in the literature (e.g. [3,4,8,10,11,18,19,25,29]). Employing this concept, some intermediate information (referred to as helper data in some work) is firstly generated based on a reference biometric template, and later, a newly-extracted template could help to recover the reference template or some relevant information if the distance between the templates is small enough (depending on the type of biometrics). Instead of employing this concept, a number of authors also suggest to compare biometric templates directly (e.g. [1,12,34]). Atallah *et al.* [1] propose a method, in which biometric templates are treated as bit strings and subsequently masked and permuted during the authentication process. Du and Atallah [12,34] investigate a number of biometric comparison scenarios by employing secure multiparty computation techniques. Schoenmakers and Tuyls [27] propose to use homomorphic encryption schemes for biometric authentication schemes by employing multi-party computation techniques.

Second, biometrics are usually regarded to be sensitive because they uniquely identify an individual. The sensitivity of biometrics lies in the fact that disclosure of biometrics in a certain application leads to the disclosure of the true identity of the involved users in this application. In addition, if the same type of biometrics of a user is used in two applications, then there is an undeniable link for the user's activities in both applications. Nonetheless, it is worth stressing that biometrics are normally considered to be public information. In [20,28,29,31,33], the authors attempt to enhance privacy protection in biometric authentication schemes, where the privacy means that the compromise of the database will not enable the adversary to recover the biometric template. Ratha, Connell, and Bolle [2,24] introduce the concept of *cancelable biometrics* in an attempt to solve the revocation and privacy issues related to biometric information. Ratha *et al.* [23] intensively elaborate this concept in the case of fingerprint-based authentication systems. Recently, Bringer *et al.* [5,6] propose a number of biometric-based authentication protocols which protect the sensitive relationship between a biometric feature and relevant pseudorandom username.

Practical concerns, security issues, and challenges about biometrics have been intensively discussed in the literature (e.g. [2,17,21,24,26,32]). Tuyls, Skoric, and Kevenaar [30] present a summary of cryptographic techniques for dealing with biometrics.

1.2 Motivation and Contributions

The stability problem concerned with biometric measurements has been paid pretty much attention and investigated very well at this moment. However,