Chapter 9
Anonymous Authentication Systems

ABSTRACT
As the first application of secure anonymous systems, after reviewing conventional schemes, this chapter develops anonymous token, ITL, and ID list based anonymous authentication systems that enable authorities to determine whether entities are eligible or not without knowing their identities. Anonymous token and ITL based systems have advantages in protecting systems from ineligible entities, i.e. different from password based systems in which eligible entities can tell their passwords to others, entities in these systems cannot give their secret to others without losing their eligibilities (in ITL based systems, entity cannot steal secrets of others). On the other hand, ID list based systems have advantages in handling entities those forget their secrets or those are expelled from systems. In the last section of this chapter, an anonymous credential system is also developed based on anonymous tags.

INTRODUCTION
Authentication is a process, in which entity S determines whether entity \( C_h \) is an authorized one or not. In this chapter, an entity that authenticates entities is called a server, and entities to be authenticated are called clients. Usually server S authenticates client \( C_h \) while identifying it. For example, a computer system authenticates users by asking them to show their identities (IDs) and passwords to protect it from being used by unauthorized persons. Namely, a user can use the computer system when it shows an ID and a password and its showing password coincides with the one that is registered with the ID in advance, therefore the computer system in this example can know the correspondences between the users and the services that the users had received from it. However, there are cases where users want to receive services without disclosing their identities. Although a restroom in an office must be protected from trespassers for safety, employees in the office may not want to show their ID and password pairs for their every use of it, because the number of times they had used the restroom, etc. are privacies of the employees, for example. Anonymous authentication mechanisms enable

DOI: 10.4018/978-1-4666-1649-3.ch009
the development of systems that cope with this kind of requirements, and constitute the foundations of almost all kinds of anonymous systems.

Here, to make authentication mechanisms practical, they must have functions to handle clients that lose their eligibilities and that forget their secrets necessary for the authentications (e.g. passwords), in addition to the basic authentication functions. Also in systems where clients are anonymous they may behave dishonestly after they had authenticated successfully, therefore it is desirable that the mechanisms can identify dishonest clients despite that they are anonymous.

Then, requirements for anonymous authentication mechanisms can be summarized as below, they are

1. Only authorized clients are successfully authenticated. This requirement is intensified to untransferability, i.e.
   a. Clients cannot give secrets necessary for authentications to others without losing their eligibilities, or
   b. Anyone cannot impersonate an authorized client by stealing or being informed of secrets necessary for authentications,
2. No one except a client itself can know the identity of the client that is being authenticated,
3. No one except a client itself can link a sequence of its past authentication requests,
4. The server can invalidate eligibilities of clients that secede from the service providing system even without carrying out seceding procedures adequately,
5. The server can handle clients that forget their secrets necessary for their authentications, and
6. Although clients are anonymous, the server can identify clients that behaved dishonestly after they had been authenticated successfully, without revealing any privacy of other honest clients.

Among the above requirements, the 3rd and the 6th requirements are not essential, but strongly desirable. Although $S$ cannot directly identify clients that had requested individual authentications even the 3rd requirement is not satisfied, a set of authentication requests from the same client suggest the identity of the client in many cases. Also, anonymous systems make entities cause various kinds of dishonest events much easier than usual systems do because entities are anonymous; therefore the capabilities of identifying dishonest clients are highly desired. Fortunately, any anonymous authentication mechanism can be made satisfy this requirement by exploiting dishonest entity detection mechanisms discussed in sections “Tokens” and “Anonymous Tags” in Part II. Namely, provided that dishonest events are detectable during clients are receiving services, $S$ can identify dishonest clients by using anonymous tokens, and by using homomorphic anonymous tokens or anonymous tag based tokens $S$ can identify them even if dishonest events are detected after the completions of services.

This chapter discusses mechanisms that satisfy the above requirements without assuming absolutely trustworthy entities. Mechanisms based on anonymous tokens discussed after the next section satisfy the above requirements except the 4th and the 5th ones. The most advantageous feature of them is about the 1st requirement. Different from password based mechanisms, in which a client can tell others its password without any damage to enable them to access the server, in these mechanisms, clients cannot give their tokens to others without losing their eligibilities. Also although any mechanism can be endowed with the capability about the 6th requirement by incorporating dishonest entity detection mechanisms discussed in Part II, anonymous token based mechanisms enable the server to identify clients liable for dishonest events without any additional mechanism provided that dishonest events are detectable during the clients are receiving services. However, the only
Related Content

Biometric Security in the E-World
www.igi-global.com/chapter/biometric-security-world/46248?camid=4v1a

Texture Recognition Using Gabor Filter for Extracting Feature Vectors With the Regression Mining Algorithm
Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore and Abhishek Kumar (2020). International Journal of Risk and Contingency Management (pp. 31-44).
www.igi-global.com/article/texture-recognition-using-gabor-filter-for-extracting-feature-vectors-with-the-regression-mining-algorithm/252180?camid=4v1a

Caught in the Web: The Internet and the Demise of Medical Privacy
www.igi-global.com/chapter/caught-web-internet-demise-medical/52368?camid=4v1a

A Framework for Protecting Users' Privacy in Cloud
www.igi-global.com/article/a-framework-for-protecting-users-privacy-in-cloud/165105?camid=4v1a