Chapter VIII
Property Protection and User Authentication in IP Networks Through Challenge–Response Mechanisms: Present, Past, and Future Trends

Giaime Ginesu
University of Cagliari, Italy

Mirko Luca Lobina
University of Cagliari, Italy

Daniele D. Giusto
University of Cagliari, Italy

ABSTRACT

Authentication is the way of identifying an individual. The techniques used to accomplish such practice strongly depend on the involved parties, their interconnection, and the required level of security. In all cases, authentication is used to enforce property protection, and may be specifically intended for the copyright protection of digital contents published on the Internet. This chapter introduces the basic concepts of authentication, explaining their relationship with property protection. The basic functionalities of challenge-response frameworks are presented, together with several applications and the future trends.

INTRODUCTION

Authentication (Greek: αυθεντικός, from "authentes" = "one acting on one's own authority") is the process of identifying an individual, merely ensuring that the individual is who he/she claims to be. Such practice is essential in networking and distributed systems, where a party has not

always the opportunity of verifying ad personam the identity of the other/s involved. The parties may be users, hosts, or processes, and they are generally referred to as principals in the authentication literature. During the authentication phase, the principals exchange messages and use the received ones to make decisions on how to act. Obviously, to prevent malicious interferences, all the messages exchanged between principals are usually ciphered. The complete sequence of ciphered messages exchanged between principals is an authentication protocol (AP). The AP can perform a mutual authentication, that is, two-way authentication, when two principals are able to suitably authenticate each other, or a one-way authentication, when only one principal is authenticated. As an example, mutual authentication refers to a client authenticating itself to a server and that server authenticating itself to the client in such a way that both parties are assured of the others' identity. Typically, this is done for a client process and a server process without any physical interaction. Challenge-response (CR) is a common AP, where a principal is prompted (the challenge) to provide some private information (the response) in order to access a service. Basically, given two principals sharing private information, that is, a secret key, CR is a one-way authentication (client-to-server) system that ensures the private information will be never sent uncrypted. However, many evolutions have been brought to the original idea. Thus, CR is a black box, whose features strongly depend on what a principal is, has, and knows. Independently from prior considerations and specifically in IP networks, an AP is intended for property protection purposes, avoiding anything in the networked/distributed system from being considered public domain and taken without permission from the creator/owner of its copyright. The objectives of this chapter are:

1. To provide essential information and strategies of existing CR frameworks, including basic hashing/encrypting techniques.
2. To focus on one of the seemingly most prolific fields related to AP: biometry applied to authentication.
3. To present a general and high-level overview of mutual image-based authentication, that is, IBA applied to this *milieu*.

BACKGROUND

This section defines the role of authentication, referring to the differences with identification, its role in the AAA (authentication, authorization, and accounting) hierarchy, its main properties and protocols, and its relationship with intellectual property protection. Specifically, the protocols are described both with common hashing/encrypting approaches and biometric features to focus on the different branches of security functions developed in the last years.

Authentication and Identification

The processes of identification and authentication are not the same practice, referring to implementation, protocols, and performances, even though the user may perceive them mistakenly as synonyms. Identification is the procedure where a unique piece of information is associated with a particular identity. It is performed by acquiring an identifier, that is, a piece of information that defines or indicates an entity, or a group of entities. Then, the process of identification is a one-to-many match test. On the other hand, authentication is the process of validating that the owning entity is really using the owned identity during interaction. Authentication is a one-to-one comparison, and could be addressed as an identification subroutine (Figure 1). A user generally claims only his/her credentials to be identified. Without his/her identity, the system searches (one-to-many search) for the profile matching with the presented credentials among a determined group of profiles and optionally performs authentication,