Chapter 5
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 work 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.

DOI: 10.4018/978-1-61350-135-1.ch005

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 from 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, *i.e.*, 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, *i.e.*, 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, *i.e.*, using the Internet Protocol, such as Internet, 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 work 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 field related to AP: biometry applied to authentication;
3. To present a general and high-level overview of mutual image-based authentication, *i.e.*, IBA applied to this *milieu*.