Authentication

I

Andrea Atzeni
Dipartimento di Automatica e Informatica, Politecnico di Torino, Italy

Antonio Lioy
Dipartimento di Automatica e Informatica, Politecnico di Torino, Italy

INTRODUCTION

In a world where computer systems are increasingly pervasive, connected and integrated, where the diffusion of electronic devices with different forms, dimensions and purposes is constantly growing, the right to protect the information exchanged through computer networks is an urgent and general need: this is known as computer and network security.

"Security" may mean different things for different people, but very often it cannot be achieved without some form of *authentication*. In particular, authentication is a cornerstone for many security operations, namely those which imply *access restrictions*, like access to personal data, separation among application of different users, process integrity and so on.

A general definition of authentication is "*the process of determining whether someone or something is, in fact, who or what it is declared to be."* In the following, we will introduce why this concept is important for the computer security field. Then, we will describe salient properties of authentication. These properties lead to an authentication taxonomy, which will be discussed with emphasis on parameters suitable for classifying different kinds of authentication. Furthermore, we will mention requirements for the authentication techniques, as well as security considerations for each authentication possibility, trying to give a comprehensive and synthetic overview of important aspects of the authentication process in practice.

BACKGROUND

Authentication is a cornerstone of computer security. It is often described as the composition of three properties: *confidentiality*, *integrity*, and *availability*:

- Confidentiality is the "property that sensitive information is not disclosed to unauthorized individuals, entities or processes." (NIST, 2007);
- Integrity is "the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner" (NIST, 2007), or even "the property whereby an entity has not been modified in an unauthorized manner" (CNSS, 2010);
- Availability is "the property of being accessible and useable upon demand by an authorized entity" (CNSS, 2010)

According to these definitions, confidentiality and integrity need a mechanism for controlling access to data and services. Confidentiality needs it to restrict information access and disclosure only to legitimate parties while integrity uses authentication to discern between proper (i.e. authorized) and unauthorized information manipulation, such as modification or destruction. Depending on the actual implementation, there can be the nice side effect of achieving also the *non repudiation* property, i.e. a party cannot deny being the author of a specific action.

Access control implementation requires both authorization and authentication. Typically, authentication precedes authorization. Although they may seem to be always combined, they are different concepts: authentication is the verification of a claimed identity while authorization is the process to verify if an entity has the right to perform a specific action on a service or resource.. For discussions and differences about authentication and authorization see (Lopez et al., 2004).

DOI: 10.4018/978-1-4666-5888-2.ch416

MAIN FOCUS OF THE ARTICLE

In this article we describe the authentication concept through its categorization on the base of different facets:

- The entity to be authenticated;
- The number of entities authenticated in the process (just one or all the involved parties);
- The meachnism (or *factor*) used in the authentication process;
- The mathematical principles exploited for authentication (i.e. the underlying cryptographic technique);
- The number of parties involved in the authentication process.

We will discuss authentication aspects along each of these dimensions.

Issues, Controversies, Problems

The set of discussion facets are typically an arbitrary choice of the authors. In our opinion, the set proposed here permits a clear depiction of the main authentication properties. However, depending on the purpose of the authentication description, other taxonomies exist.

For example, in (Simmons, 1988) the proposed authentication taxonomy objective is to point out and discuss two authentication goals: 1) to verify that the information was, in all probability, actually originated by the purported originator, 2) to verify the integrity of the information, i.e. to establish if the message was originated by the authorized source and it hasn't been subsequently altered, repeated, or delayed. Simmons' classification significantly differ from our since it adopts Information Theory concepts (Shannon, 1949), thus approaches the problem from a theoretical point of view.

Another example of taxonomy (Lowe, 1997) introduces several possible definitions of authentication. Each of them is discussed and formalized using the process algebra in order to study their relative strengths. The goal in this case is to characterize authentication in a way manageable by a model checker, to allow formal verification of authentication protocols (Cremers et al., 2009).

In the next section we will describe our interpretation of authentication characteristics. These attributes deviate from those in previous categorizations since our goal is to give a widespread understanding of current authentication trends. For different targets – such as formal verification – a different (e.g. more analytical) classification can better fit the purpose.

Solutions and Recommendations

Entity to be Authenticated

In the general case, the entity to be authenticated can be a data chunk (e.g. a network packet or a file) or a communication entity (e.g. a human operator or a network server). In case the entity to be authenticated is a data fragment, we talk of *data* or *origin authentication,* in case the authentication target is a communication entity, we refer to *peer authentication.*

Data authentication is related essentially to the integrity security facet, and is commonly defined in a communication exchange, as the process to verify that the data received have been created by the sender, which also implies no unauthorized data modification occurred.

On another hand, peer authentication, sometimes named *peer-to-peer authentication* or *peer entity authentication,* indicates the process that provides proof of the communication peer's identity in the setup phase of a data connection (and possibly, verified again during the data transfer phase). The purpose is to detect an entity attempting to impersonate a different peer in the communication. Ideally, this should avoid the malicious entity to provide wrong data (by forging unauthorized ones or by improperly replaying originally authorized ones) or to acquire unauthorized information.

Entities Authenticated in the Process

In a network communication between two peers, the authentication process is named *simple* if only one of the two entities has to provide proof of its identity. When both entities have to prove each other their identities then the process is named *mutual authentication*.

Depending on the scenario requirements, simple authentication can provide enough security. For example, if a peer is looking for public information (e.g. through a newsfeed service), the security needs are