Chapter 8
An Examination of Identity Management Models in an Internet Setting

Kenneth J. Giuliani
University of Toronto Mississauga, Canada

V. Kumar Murty
University of Toronto, Canada

ABSTRACT

The purpose of this chapter is to examine the strengths and weaknesses of the most commonly used model for digital identities. It is compared to other models which have preceded it, thus giving a background on its development. The models are measured against a set of criteria which it is desirable for an identity management system to have. The underlying hope is that understanding this model will help improve it or even lead to a different model.

1. INTRODUCTION

As more and more websites arise on the internet every day, users now have an incredible amount of possible activities available to them. However, the sheer volume of these possibilities comes with its share of challenges.

One of the key problems that exists on the internet is that of entity authentication. It is essential that the parties involved in any transaction be sure that the entities they are communicating with are indeed who they say they are. Failure to do so can lead to fraud, disclosure of private information, or many other undesirable consequences.

To solve this problem, many internet sites require a user to log in using a userid and password. While theoretically effective, the proliferation of websites has made this paradigm highly inconvenient.

Quite often, users will choose passwords to be too short, easily-guessed, or will use the same password for multiple sites. This has given rise to the recent phenomenon of password fatigue.

In addition, with the great diversity of transactions that may take place comes varying levels of

DOI: 10.4018/978-1-60960-123-2.ch008

personal information which needs to be transmitted. It is imperative that the information not only gets to its desired destination securely, but that the right kind of information is transmitted.

One solution that has been proposed for this is the use of digital identities. Digital identities allow entities to uniquely identify themselves to other parties on the internet. In this way, they can bypass many of the problems associated with the userid/password paradigm.

In this paper, we examine the current model used for digital identity management in detail. In order to do so, we first examine models previously used, either theoretical or practical, to give a background on how the current model evolved to its present point. We examine its strengths and weaknesses. We also establish a set of criteria which are desirable for an identity management system to have.

2. PRELIMINARIES

The phrase *identity management* can take on many different meanings. Birch and David (2007) gave good introduction into the subject. For the purpose of this paper, however, we will restrict ourselves to the management of digital identities in an internet setting. More formally, we define *identity management* to be the set of processes, protocols, and policies which deal with digital identities. A digital identity consists of a set of elements including an *identifier*, a unique string which is bound to a specific user and *attributes* associated with that identifier. For example, an e-mail address or a userid can be considered as identifiers. An *identity management system* is the architecture that defines the mechanisms related to the interaction of parties using digital identities.

3. THE TRADITIONAL MODEL

The traditional model for internet transactions involved two parties:

- **A user:** a person who makes use of the services in an online environment,
- **A relying party:** an entity which provides a service on the internet, normally but not restricted to being a website.

The main transaction will occur between the user and relying party. As a practical example, the user may be an individual and the relying party a website such as an online bank or store. In this context, transactions will be initiated by the user. Furthermore, the biggest challenge will be for the relying party to authenticate the user.

We note here that relying party authentication should also be considered since spoofing or phishing attacks or malicious relying parties are also possible.

A typical transaction between the two parties is shown in Figure 1.

Figure 1. Transaction in the traditional model