Chapter XIV
Authentication and Access Management of Electronic Resources

Juan Carlos Rodriguez
California State University, Sacramento, USA

Bin Zhang
California State University, Sacramento, USA

ABSTRACT

This chapter opens with a discussion of the varying needs of libraries to provide their users with both local and remote access to electronic resources within the context of the various legal and technical issues surrounding them. An overview of the various types of authentication and authorization mechanisms currently in use by libraries, their parent organizations and electronic resource providers is presented. Further discussion follows on the unique needs and requirements of consortia licensed electronic resources and metasearch applications. The chapter concludes with a look at future considerations and directions libraries and e-resource providers may take with regard to secure and seamless access to electronic resources.

INTRODUCTION

As late as the early 1990's, the library's primary method of access management to its collections was either performed at the library's entrance or through the use of publicly inaccessible collections or "closed stacks" that required some form of permission or authorization to access them. Additional access management was introduced when it came time to borrow the library materials from the library. Typically this was done by requiring the library patron to present a valid and current library card that was issued to them as a member of the community, a faculty member, or student of the university. Also, most libraries were not concerned with providing remote ac-

cess to their collections since they still existed primarily in physical form and all access was limited to in person. With the introduction of online electronic resources such as electronic journals and online databases, these traditional methods of access management became no longer sufficient. It was no longer possible just to control access through physical methods, additional methods were needed.

Over the past ten years, the amount of licensed electronic resources purchased by libraries has increased dramatically. During the period from 1995 through 2005 the average Association of Research Libraries (ARL) library's allocations of financial resources devoted to electronic resources (e-resources) had increased from a little more than 6% to almost 38% of the library's entire collections budget (Kyrillidou & Young, 2006). The bulk of these resources have been electronic journals and index and abstracting databases. Included in most, if not all, of the license agreements is the need to restrict access only to those that are members of the library community. For academic and special libraries this community generally consists of its faculty, staff and students. However, it's much more difficult to identify a public library's community considering most members of the community served by a public library, and often residents of the state, are potential members of this community. For this reason access to electronic resources is typically restricted to computers that are physically in the library while remote access is generally provided to those that posses a valid library card.

Initially the use of passwords that were given to libraries from e-resource vendors to distribute to its users was the primary mechanism for providing access to e-resources licensed by the library. However as the amount of e-resources and vendors grew, so did the workload in managing passwords. This method quickly became a growing concern and problem for libraries. As a result, the ability to restrict access to a particular physical network location through the use of IP address filtering soon became the de facto standard on how access was managed. An IP (Internet protocol) address is a unique string of four numbers separated by periods (such as 216.230.155.100) that is assigned to a device, such as a computer, connected to the Internet. Typically computers in a library or university have IP addresses that fall into a common range. For example, a public library may have five Internet-connected computer workstations that have the following IP addresses: 216.239.255.101; 216.239.255.102; 216.239.255.103; 216.239.255.104 and 216.239.255.105. In this example, all five workstations share the same first three strings (i.e. 216.239.255) of numbers. IP address filtering is a method where the vendor only accepts requests that originate from registered networked computers that fall within the range of IP addresses that the library has supplied the vendor. Again, this method quickly became restrictive as more and more users began requesting access to these resources remotely. Thus there became an increasingly important need to implement mechanisms that addressed licensed restrictions while at the same time meeting the needs of both local and remote users.

This chapter will explore the various mechanisms that are currently in place that provide both authentication and authorization for the variety of library licensed electronic resources. It will address issues related to the legal, technical and privacy issues associated with providing local and remote access to licensed resources.

BACKGROUND

When a library decides to purchase an e-resource it must also consider the methods that it will use to provide access to these resources. Typically, most e-resources are available for access from the vendor. Since many pricing models for electronic resources factor in the size of the user base, the vendor of the electronic resource requires that access to the electronic resource be restricted only