Chapter 6
DRM Protection Technologies

Gary Hackbarth
Northern Kentucky University, USA

ABSTRACT

Digital Rights Management (DRM) is concerned with the ownership of digital information and access to that information. Organizations and individuals increasingly seek to prevent unauthorized or inadvertent release of owned, proprietary, or sensitive information. A variety of technologies are available to prevent the piracy and verify the true owners of digital content, unfortunately specifics of these technologies are often proprietary. Content can be protected by a variety of encryption techniques for the storage and transmission of digital information yet; these same techniques can limit access and usability of digital content. This chapter discusses the general state of digital security and technologies in use followed by a discussion of future directions for digital security research and practice.

INTRODUCTION

Information or data security is the general means of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Organizations develop security policies to clearly articulate the specific rights and responsibilities of individual users, and to communicate these rights successfully to each employee so that there is an effective approach to information security across the organization (Doherty et al., 2009). The terms information security, computer security and information assurance are used interchangeably by the public because they share the common goals of protecting the confidentiality, integrity and availability of information. More specifically, (1) Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms; (2) Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer; and (3) Information Assurance (IA) is the practice of managing information-related risks (Alexei, 2006; D'Aubeterre, et al., 2008; Jean-Noel, et al., 2007).

DOI: 10.4018/978-1-4666-2136-7.ch006

It is important to understand that these fields overlap in that they confront the same issues but use different methodologies and techniques to address security issues from a different perspective. More specifically, a related issue to all three sub-disciplines is the issue of Digital Rights Management (DRM). DRM is a generic term for access control technologies that can be used by hardware manufacturers, publishers, copyright holders and individuals to try to impose limitations on the usage of digital content and devices (Fetscherin, (2002). The term is used to describe any technology which inhibits uses (legitimate or otherwise) of digital content that were not desired or foreseen by the content provider.

In reality, for most people, digital security just exists. There exists an expectation that digital content will arrive at a computer, be delivered to their TV, or heard on their radio. There is an expectation that personal information will be protected by financial institutions, business entities, educational institutions, the government, and others trusted with the responsibility of guarding intellectual and personal information. There is little thought given to the hackers who seek to capture and reuse digital content for their own profit. For most of us, safeguards that protect or help deliver digital content are something that happens in the background. Furthermore, many users assume the digital content downloaded to their personal device (TV, iPod, Computer, etc,) is free. The reasons for this assumption are complex but relevant to businesses trying to develop pricing schemes/strategies and product delivery models needed to sell digital content.

When we hear about identity theft, digital piracy, illegal copying of songs or other instances of digital abuse of protected information, we consider it an issue for law enforcement, security experts, or the businesses and people involved. Many IT professionals feel the same way. Digital security is about complicated algorithms, high-tech hardware, and complex communication configurations. The purpose of this chapter is not to convince you that digital security is important but rather to inform and instruct readers about the available technologies and issues required in managing digital rights.

BACKGROUND

Digital media is replacing analog media as the primary technique in the way data or information is stored, transmitted, and used. The advantage of traditional analog information or other forms of traditional informational content (books, taped video, microfilm, records, etc.) is that it is relatively difficult and expensive to create high quality copies of the original materials. To this extent, traditional copyright law worked (Bates, 2008). As media shifted toward digital formats, the cost of reproduction declined and the capability to create exact high quality duplicates evolved. Under these circumstances, the protections given to authors under traditional copyright law begin to breakdown.

Copyright in the context of this chapter is intellectual property that gives the author of that intellectual property, exclusive right for a certain period of time to control publication, distribution, and adaptation of the original work, after which time the original work is released to enter the public domain (Crane, 2009). In general, copyright law applies to any expressible form of an idea or information that is substantial, is discreet in that it has a beginning and an end, and is complete in some final form. Complicating copyright law is that while there are some international standards, copyright law does vary by country. Internationally, copyright standards exist for the author between 50 and 100 years from the author's death or for a shorter period of time. Further, some international jurisdictions require administrative action to establish copyright, but most countries recognize any completed work. In general, copyright is a civil matter, although,