Measures To Enforce Safety In Digital Libraries

Tadakamalla Sekhar, A.V.L.V Prasad Rao, K.P.R Krishna Chaitanya
Librarian, Anurag Pharmacy College, sekhartadakamalla@gmail.com,
Librarian Anurag Engineering College, anuraglibrary@gmail.com,
Asst.Proff. Dept.of C.S.E,krishnachaitanya.kpr@gmail.com
J.N.T.U Hyderabad.
Anurag Engineering College
Ananthagiri(v),Kodad,Nalgonda,A.P,India.

Abstract:-The Digital Library System is an Innovation in Library Service. It is prone to Onslaughts of sabotage by Bibliophiles, Bibliophobes and Biblioklepts all alike the system itself inherent facilities which render it susceptible to the forays and ravages of the users. The Management of digital library has to be watchful wary and chary in order to avert possible embarrassments. The Digital Library Manager has serious concerns in providing protection to the Noetic wealth. The conflicting needs make the problem all the more complex. A Holistic vision alone can handle the conflicting situations. The Inherent weaknesses of the Digital Library system expose it to deleterious detriment as well as detritus. The security attacks may be categorized as physical attacks and Logical attacks. A physical attack involves security of Hardware – Keys, Locks, Cards and Visitor monitoring. A logical attack involves the abuse of the content of the Digital Library much due to the detriment of Intellectual Property and Authenticity. This paper focused on two aspects i.e., Content, Users.


1. Introduction

1.1 Security Issues with Digital Libraries

According to the DELOS Reference Model [2](Candela et al., 2007), there are six main concepts in a digital Universe. Content, Users, Functionality, Architecture, Quality and Policy. Each of these concepts has security issues that affect it.

1.2. Content

The content of a digital library includes the information objects that a digital library provides to the users. Some of the security issues involved are integrity and access control[3]. Integrity requires that each object/resource has not been altered or changed by an unauthorized person. Access control encompasses two security requirements. The first is authentication[4] where the user must log into the system while the second is confidentiality, which means that the content of an object is inaccessible by a person unless they have authorization. Not all Digital Libraries are free; often content is provided to Digital Library users for a certain fee, whereupon access control is needed to protect the content. Further, some content is inappropriate for some users, or targeted to particular user groups; there are a whole host of such other reasons for access control. Logical attacks such as hacking and message tampering can affect the integrity and confidentiality of the content. Improved information access in digital libraries has raised many issues that affect the management of digital libraries. Content Management, or more specifically Digital Rights Management, refers to the protection of content from the different logical security attacks and issues relating to intellectual property rights and authenticity.

2. Digital Rights Management

DRM provides content protection by encrypting the content and associating it with a digital License (Tyrväinen, 2005). The License identifies the user allowed to view the content, lists the content of the product, and states the rights the user has to the resource in a computer readable format using a digital rights expression language [6](DREL) or extensible Rights Markup Language[5](XrML) that also describes constraints and conditions. There are 7 technologies used to provide DRM. Table 1 summarizes the DRM components and supporting technology. Each of these components involves mechanisms used to provide DRM:

• Encryption:

Techniques such as symmetric and asymmetric ciphers can be used to provide access control; public-key encryption is used in payment systems that control how and by whom the content is used. Symmetric ciphers using DES, 3DES,
AES, and RC4 algorithms [8] require the use of a shared secret key to encrypt data before it is sent. At the receiver’s end the cipher text is decrypted using the same secret key. Symmetric ciphers depend on both the sender and receiver knowing the shared key. Asymmetric ciphers [9] use a pair of keys, public and private, for each of the sender and the receiver. The public keys of both the sender and the receiver are known but the private key is kept secret. If encryption is performed using the public key then only the private key can be used for decryption and vice versa.

• **Passwords**: Stored strings must be matched by users desiring access.

• **Watermarking**[10]: Characters or images are added to reflect ownership. Steganography is used to conceal data inside audio, video, or images (Johnson & Jajodia, 1998). Different watermarking techniques have different aims; some watermarks might be visible while others invisible. Some watermarks are reversible (Mintzeret al., 1997); it depends on the desired use of the watermark and what is being protected.

• **Digital signature**: Asymmetric encryption [11] can be used. Likewise, hash algorithms such as MD5 and SHA[11] can be used to create a signature (Stallings, 2006).

<table>
<thead>
<tr>
<th>Component</th>
<th>Protection Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access and usage control</td>
<td>Encryption (e.g., symmetric, asymmetric), passwords</td>
</tr>
<tr>
<td>Protection of authenticity and integrity</td>
<td>Watermarks, digital signatures, digital fingerprints</td>
</tr>
<tr>
<td>Identification by metadata</td>
<td>Allows description of an object in suitable categories, covering the digital content, rights owner, and conditions.</td>
</tr>
<tr>
<td>Specific hardware and Software</td>
<td>Includes all hardware and software used by the end-device through which the digital content is being played, viewed, or printed.</td>
</tr>
<tr>
<td>Copy detection systems</td>
<td>Search engines, which search the network for illegal copies and use watermarking.</td>
</tr>
<tr>
<td>Payment systems</td>
<td>Can be seen as a certain type of protection technology as it requires user registration, or credit card authentication, which also require a trust relationship between the content provider and the customer.</td>
</tr>
<tr>
<td>Integrated e-commerce Systems</td>
<td>DRMS must include systems which support contract negotiation, a counting information, and usage rules.</td>
</tr>
</tbody>
</table>

Table 1. DRM Components and Protection Technologies, adapted (Fetscherin&Schmid, 2003)

• **Digital Fingerprint**: Digital fingerprints are a more powerful technique involving digital signatures and watermarking. The creator of the content creates a unique copy of the content marked for each user; the marks are user-specific hence called fingerprints. Should a user illegally distribute the content, the creator can use search robots to find those copies (Schonberg & Kirovski, 2004).

• **Copy Detection Systems**: Search engines also can help locate such copied objects. Copy-detecting browsers can protect digital content too.

• **Payment Systems**: Users must divulge personal information to pay for content. Installing payment systems can help protect digital content. There is no standard mechanism for providing DRM, mainly due to the lack of regulations, however there are various systems and protocols introduced to provide content management and support fair usage policies. There is a tradeoff between security and performance. Nadeem and Javed use a Pentium-4, 2.4 GHz machine running Microsoft Windows XP operating system, encrypt 20527 bytes to 2323398 bytes of data using DES, 3DES, and AES. For 20527 bytes of data it took 2 seconds to encrypt using the DES algorithm and 4 seconds to encrypt using the AES.
The various attackers monitor network traffic to intercept passwords. It secures communication, provides single sign on and mutual authentication, and does not send a user’s password in the clear on an insecure network. An alternative solution suitable for digital libraries (Winslrett et al., 1997), is to represent information about an individual using credentials. Credentials are “abstract objects which contain statements expressing knowledge or information from a definite context.”

3. Summary
Digital libraries should be secure. This is an important quality that affects all aspects, as has been shown above using the DL characterization of the DELOS Reference Model (Candela et al., 2007). We also can summarize and elaborate upon this point using another framework for DLs (Gonçalves et al., 2004). The SS framework supports Societies and their needs, covering all aspects mentioned above about Users and related Policies, as well as Quality (Gonçalves et al., 2007). Since Societies cover software actors, agents, components, modules, etc., this also encompasses related Architectural issues. Thus, security with regard to Societies covers issues like client/server, commerce, identity, peer-to-peer, privacy, rights, roles, teams, and trust. Scenarios cover functions, operations, requirements, services, and tasks. Examples (Gonçalves et al., 2008) include access, access control, authentication, browsing, copying, denial of service attacks, encryption, payment, recovery, searching, usage, and watermarking.

4. References


The DELOS Digital Library Reference Model:
http://www.delos.in fo/index.php?option=com_content&task=view&id=345


Introduction to Digital Libraries, Facet Publishing:


[1] Digital Library Manager
http://kered.org/blog/2008-02-07/gpapers-a-digital-library-manager/

ue&id=345/
http://strathprints.strath.ac.uk/13045/
http://oc.ac.ge/mod/resource/view.php?id=197

http://en.wikipedia.org/wiki/Access_control_list

http://en.wikipedia.org/wiki/Authentication
http://searchsecurity.techtarget.com/definition/authentication
http://www.rsa.com/glossary/default.asp?id=1006

http://en.wikipedia.org/wiki/XrML
http://searchsoa.techtarget.com/definition/XrML

http://jweblv01.jisc.ulcc.ac.uk/media/documents/techwatch/tsw0603.pdf

[7] Encryption
http://searchsecurity.techtarget.com/definition/encryption
http://www.howstuffworks.com/encryption.htm

[8] RC4 Algorithm
http://en.wikipedia.org/wiki/RC4


http://www.codeproject.com/Articles/5068/RC4-Encryption-Algorithm-C-Version

[9] Asymmetric cipher
http://en.wikipedia.org/wiki/Public-key_cryptography
http://www.windowsitpro.com/article/security/symmetric-vs-asymmetric-ciphers
http://en.wikibooks.org/wiki/Cryptography/Asymmetric_Ciphers

[10] Watermarking
http://en.wikipedia.org/wiki/Watermark
http://www.jjtc.com/Steganography/

http://hitachi-id.com/concepts/asymmetric_encryption.html
http://searchsecurity.techtarget.com/definition/asymmetric-cryptography

[12] MD5 and SHA
http://www.secure-hash-algorithm-md5-sha-1.co.uk/
http://en.wikipedia.org/wiki/SHA-1

http://en.wikipedia.org/wiki/Access_control
http://www.computer-network-security-training.com/what-are-access-control-models/

[14] Kerberos
http://web.mit.edu/kerberos/
http://searchsecurity.techtarget.com/definition/Kerberos
http://www.ietf.org/rfc/rfc4120.txt