ACCESS PROVISION AND SECURITY TO DIGITAL RESOURCES

By

Mukut Sarmah*
Sumana Chakraborty**

ABSTRACT

Usage of digital media has witnessed a tremendous growth during the last decades, as a result of their notable benefits in efficient storage, ease of manipulation and transmission. However these features make digital media vulnerable to copyright infringement, tampering and unauthorized distribution. The access provisions and security or protection of digital resources has received significant attention within the digital media community, and a number of techniques in this respect have been evolved. In this paper we have discussed some of the reasons for attacking the digital resources; authentication, authorization, data hiding techniques for copyright protection and also some relevant topics of research results.

---

* Librarian, Pandu College, Pandu, Guwahati – 12; E-mail: pclib@gw1.dot.net.in
** Information Scientist, Tezpur University, Napam; E-mail: scs@agnigarh.tezu.ernet.in

0. Introduction

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. In a digital library, digital audio/video/images and multimedia documents can be stored efficiently with a very high quality and manipulated easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks. Actually, digital libraries are network based distributed systems, with individual servers responsible for maintaining local collections of digital documents.

The easy transmission and manipulation of digital data constitutes a real threat for information creators and distributors e.g., news agencies, museums, libraries, artists, scientists, authors of multimedia documents etc. Copyright owners want to be compensated every time, their work is used. Furthermore, they want to be sure that their works are not used in an improper way e.g., modified or edited without permission. However when it comes to digital data, copyright enforcement and content verification are very difficult tasks. One solution would be to restrict access to the data using some encryption technique. But encryption does not provide overall protection. All forms of digital data (still images, audio, video, text documents, multimedia documents) can be used for information hiding. In the following pages, we shall discuss some of techniques used for the same purpose to have a secured digital library system.

1. Attack issues

An attack is an unauthorized action undertaken with the intention of hindering, damaging, incapacitating or breaking the security of the server. The attacks may broadly be categorized into two types:

1.1 Active attack:

In active attack, the intruder directly enters into the network system and damages or changes the programme or software or information running through that network by any user.

1.2 Passive attack:

In passive attack, the intruders are able to damage information from network but they only come to know about some scaled information, which is not supposed to read be or listened to by them.

1.3 Why attacks:

There are many reasons why the intruders break network security. Some of the reasons are spite, sport, profit, stupidly, curiously, politics, etc. There are various categories of people who attack network for various purposes. Students attack for having fun, hackers to test out someone's security system. Businessmen for discovering competitors marketing plan, stock brokers to deny promise made to a customer by e-mail, spies to learn on enemy's military strength and so on. So, to overcome the various attacks or to maintain network as well as other digital materials, security enforcement is a must. We, therefore, have to concentrate ourselves on authentication.

2. Authentication

This term is used in verifying the users as well as the resources. It is the process that checks the integrity of transmitted data, especially a message. Thus, we can get two types of authentication:

2.1 Users authentication.
2.2 Resources authentication.
2.3 Users authentication:

Users authentication relates to the users of the documents. There are three types of users authentication.

- 2.1.1 By knowledge.
- 2.1.2 By ownership.
- 2.1.3 By characteristics.

2.1.1 By knowledge: It relates to the password. This means that the password is in the knowledge of the users himself or herself. No other person knows it if the owner does not tell it. When, the password is known by other person, there is nothing secret, and it is no longer a method of authentication.

2.1.2. By ownership: These relate to the identity card, smart card, etc., for some users. He/she owns an identity card/smart card as a proof of his/her authenticity or authorization.

2.1.3. By characteristics: It is another method of authentication. A particular characteristic of a person shows his/ her authentication. e.g. finger print, retinal pattern, DNA, etc.

Now, if we consider any one method from above, our assumption may be wrong. For example, if there is a provision for giving finger impression in the computer, or any other image, then sometimes it may happen that a simple photograph can betray us instead of a real human being. So, simply any one method is not sufficient for authentication.

If we combine two methods, suppose, A and B or B and C or C and A, it becomes a bit stronger, but the combination of A, B and C makes it strongest. Thus, security and authenticity is a set of A, B and C.

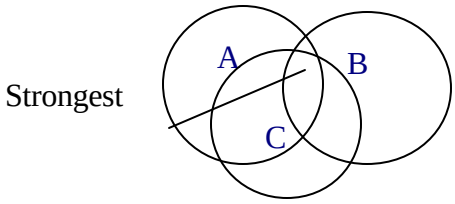

Fig. 1. Security and authenticity using A, B and C

2.4 Resource authentication:

Cryptography can be used in a number of ways to keep information private and provides a framework for secure message exchange and transmission. Digital signatures and digital certificates are used to prove the authenticity of document content.

2.4.1. Digital Signature: It enables the recipient of a message to authenticate the message and verify that the message is intact as it was sent. If a user asks for it, the sender does the same. Thus, digitally signed document gives a legal standard. A hand written document can be counterfeited easily. Moreover, the signatory can repudiate the signature claiming it was counterfeited. Digital signature is almost impossible to counterfeit.

The signature can be produced by using a one-way function i.e. by an encryption technique. It converts a message of any length into a fixed length message digest called hash or message digest. There are a lot of hash functions, e.g. Secure Hash Algorithm (SHA), developed by National Institute of Standards and Technology (NIST).

2.4.2. Digital ID or Certificates: There are some organizations called Certificate Authorities, to let us know about the authenticity of a certificate. Actually, certificates are nothing but the package of information signed by a Certificate Authority. The certificate authority maintains a hierarchy. A 'local CA', which certifies some local users, again can be certified by a 'state CA', which is again certified by a national CA and so on.

3. Authorisation

Authorization is the granting of access rights to a user, programme or process. A library is there to serve all users. But, we find some sort of restrictions in the libraries. There are different categories of library for some specific category of users. e.g. academic library, special library, etc. So, from the very root, we get the concept of access provision as well as access control. The students, teachers and employees of a particular institution can use their library. They must be bonafide members.

3.1 Access provision or privilege:

Privilege means the types of accesses to the digital resources i.e., read, write, edit, etc. How much access provisions one possesses, depends upon the organization, system of using of the digital resources etc. It may vary depending on various factors viz. the job category, authenticity of the information, proprietary rights, etc. We can minimize or maximize the access provisions by controlling it.

3.2. Access control:

Access control in a digital library means to provide a limitation to the access of all users to all information of the library. It helps in protecting the network resources, files, data, audio-visual materials, databases, etc. Access control is one of the most important services for network security. It is very close to security, authenticity, and authorization of the users. Every digital library must have this mechanism for protecting the network resources, and its various services. Based on access control mechanism, we can categorize these into three different types:

3.2.1 Mandatory Access Control (MAC)
3.2.2 Discretionary Access Control (DAC)
3.2.3 Role Based Access Control (RBAC)

3.2.1 MAC: MAC is a set of rules applied globally to the security policy. It is implemented for network users and resources too. MAC is used when there are identifiable information categories. For identification of information and users MAC can be implemented. It is called MAC (Mandatory Access Control), because labeling of information happens automatically and can not be changed or modified by general user community.

3.2.2 DAC: It depends on user identity or group membership. It is called discretionary, because a file owner can change its permission. A DAC permission on system files can

only be changed by the administrator who owns them. DAC involves being able to completely control, which file and resource a user may access at a given time. That means the administrator or owner of the file will give the authority to others. DAC is the technology that has trickled down from defence sources. In defence organisation, the administrators must be concerned about the authorized personnel regarding their access provision.

3.2.3 RBAC: There is another more important access control system, which is called Role Based Access Control. It is a technology that is attracting a large number of people particularly for commercial applications because of its simplicity. One of the most challenging and important problems in a network system is maintenance of proper security administration. Different organizations are there for managing the security in distributed multimedia environments.
Security administration is costly and prone to error because, administrators usually specify access control lists for each user on the system individually. Access control lists are those, which are used to maintain a list of all individuals or processes that are authorized to access specific information, applications or network resources. These are most common forms for accessing into the networks today.

4. Confidentiality

Confidentiality is nothing but the provision for keeping privacy for the messages and storing the data by hiding information using encryption techniques.

If we want to keep something private we are to hide it from others. When we send some confidential message to others we always want to keep it secure so that no one can break the seal and read the message. So, for these types of situations, we are to maintain some sort of confidentiality. In the present era of information explosion, we are using Internet, e-mail etc. always, for transferring or disseminating information. So, for secret messages we are to follow the paths for solution i.e. encryption. The term encryption comes under cryptography. Cryptography is the art of hiding and securing information for storage and transmission. In cryptography the readable text is written in a code, which does not allow others to read the text. This process of conversion is called encryption. The message to be encrypted is called plaintext; the process for reverting the encrypted information is called decryption and the output information is called cipher text. In one encryption method, one key is kept secret, which enables the message to be sent to the recipient secretly. As one key is kept secret, the technique is often called symmetric or single key or secret key cryptography.

But in this process, a problem arises when somehow, the secret key is made public by some intruders. So, to maintain better and more security, Whitfield Diffie and Martin Hellman developed the concept of public key encryption, or asymmetric encryption, which is quite effective.

5. Protecting intellectual property

With the growth and advent of digital information, the illegal distribution and duplication of data as well as information takes place to a greater extent. As other unauthorized party or person duplicates the digital information, so, the need for effective copyright protection tools is demanded. Various attempts are being made by software companies to develop their own software so that the information, it may be audio, visual, images, etc. can be protected in their respective files.

5.1. Digital watermarking:

A digital watermark is a label embedded to the digital data or information (like audio, video, still images, etc.), which can be extracted later to make an assertion about the data. The extraction is done through computing operations. A digital watermark is used to identify the source, creator, owner, distributor, and authorized consumer of the document. A watermark is given to a document to give a permanent seal so that it cannot be copied and mishandled.

5.1.1 Applications: Digital watermarking can be applied for various purposes:

5.1.1.1 For ownership assertion: The owner of document (e.g. image) can watermark on the same and make the document publicly available. He/she keeps the original document with himself/herself. But later on, when required, they can prove it with the original image.

5.1.1.2 Fingerprinting: Unauthorized distribution of publicly available multimedia content can be avoided by using watermark.

5.1.1.3 Authenticity verification: When multimedia contents are used for legal purposes, the originator of the content is to prove it. Watermark acts as an authentication key for the originator.

5.1.1.4 Access control: Access to data can be controlled for some contents.

5.1.1.5 Content protection: In certain applications a content owner may want to publicly provide a preview of the multimedia content. Then the content owner can watermark it, so that it can not be commercially used by others.

5.1.2 In case of watermarking, we find mainly three different types. They are –

- Invisible watermarks
- Visible watermarks.
- Dual watermarks.

5.1.3. Present technology: In respect of security, we find various technologies to be evolved. They are DES, S-HTTP, , SSL, IPV6 etc.

5.1.3.1 DES (Data Encryption Standard) was originally developed by IRM, US. DES is a secret key, symmetric cryptosystem. When DES is used for communication, the sender and receiver both must know the same secret key, because it is used to encrypt and decrypt the message. It is beneficial for large set of data. One should change DES keys frequently, to prevent attacks that require sustained data analysis. In a communication system the sender and receiver must find a secure way to communicate the DES key to other.

5.1.3.2 (S-HTTP) Secure Hypertext Transfer Protocol was developed by Enterprise, Integration Technologies, a division of Verifone, part of Verifone's Internet Commerce Division. Secure HTTP is an extension of HTTP. It provides independent applicable

security services for transaction confidentiality, authenticity, integration and non-rapid ability of origin.

5.1.3.3 SSL (Secure Socket Layer) is a system designed and proposed by Netscape Communications Corporation. SSL protocol supports a wide range of authentication scheme. The SSL protocol is composed of two layers. The goal of SSL is to provide privacy and reliability between two communicating applications.

5.1.3.4 IPV6 is a short form for "Internet Protocol Version6". It has been designed by IETE (Internet Engineering Task Force) to plan the current version of Internet Protocol. Most of the Internet users today use IPV4, which is almost twenty years old. Many common Internet applications are already working with its latest version IPV6.

6. Conclusion

A digital library is meant to allow universal access to all citizen to reach to all kinds of information. The users have the provision to access the digitized materials like e-journals, CD-ROM, various files through Internet, various databases of books, journals etc. But if all people have free access provision to all information, then there may take place some unwanted happenings because of fun, revenge, theft, enmity, etc. Some locally and unavailable materials are often damaged by intruders. A digital library service must protect its digital sources against the misuse of their contents by various intruders.

Hence, we must maintain and implement some security policy in the digital libraries. Various security techniques like password, users identity card, hierarchy card methods for access control etc. should be adopted for the benefit of users and institutions. Moreover, in the network systems of computers various techniques like encryption and decryption key systems, watermarking techniques etc. are used as a key for authentication as well authorisation.

7. References

Web sites:

1. http://www.csrc.nist.gov/nistpubs/800-7/node44.html
2. http://www.dlib.org/dlib/december97/im/12lotspiech.html
3. http://www.dlib.org/dlib/june97/ibm/06gladney.html
4. http://www.doc.sco.com/sec-audit/access-control-events.html
5. http://www.garrison.com/html/docmacdac.html
6. http://www.hissa.nist.gov/rbac/
7. http://www.nwfusion.com/newsletters/sec/0103secl.html

Books and Journals:

1. Ackermann, Ernest. Learning to use the Internet: an introduction with examples and exercises. New Delhi: BPB, 1996.
2. Furht, Borko; ed. Handbook of Internet and Multimedia: system and application, Floriada: IEEE Press, 1999.
3. Happell, Laura. Novell's guide to Netware LAN analysis. New Delhi: BPB, 1993

4. Jordan, Larry and Charchill, Bruce. Communications and Networking for the PC. New Delhi: Prentice hall, 1996
5. Memon, N and Wong, P. W. Protecting digital media content, Communications of the ACM, Vol. 41(7), July, 1988.
6. Moorthy, A. Lakshmana and Karisiddappa, S. Electronic publishing impact and implications on library and information centers in digital libraries. In: Dynamic store house of digitized information, New Delhi: New Age, 1996. pp. 15-35.
7. Nance, Barry. Introduction to Networking. 4th Ed. New Delhi: Prentice Hall, 1998.
8. Poulter, Alan; Treng, Gwyneth and Sargent, Goff. The Library and information professional's guide to the World Wide Web. London: Library Association, 1999. pp. 1-33.
9. Prakash, B. P. Digital Imaging: technology, trend and impact on libraries. In: Dynamic storehouse of digitized information, New Delhi: New Age, 1996. pp. 51-61.
10. Saknure, B. G. Digital libraries vs. conventional libraries. In: Library vision 2010: Indian Libraries and Librarianship in retrospect and prospect. Seminar papers, All India Library Conference(45th:1999:Hisar) edited by Prof. J. L. Sardana, New Delhi: ILA, 1999. pp. 151-58.
11. Stallings, William. Cryptography and network security: principles and practice. 2nd Ed. New Jersy: Prentice Hall, 1995.
12. Tanenbaum, Andrew S. Computer Networks, 2nd Ed. New Delhi: Prentice Hall, 1996.
13. Waltham, Tony. Warehouse on the Net. In: Computers Today. Vol. 16(207), July,16-31, 2000, pp. 58-59.