IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4585

# Enhancing E-Learning with a Document Control Environment

**Ajin Jirachiefpattana, Ph.D.**
Department of Computer and Statistics, Faculty of Arts and Sciences, Dhurakijpundit University
Laksi, Bangkok 10210 Thailand., Tel: (66 2) 9547300-29 Ext. 257, Fax: (66 2) 5899605-6
Email: ajin@dpu.ac.th

**Waraporn Jirachiefpattana, Ph.D.**
School of Applied Statistics, National Institute for Development and Administration
Bangkapi, Bangkok 10240 Thailand, Tel: (66 2) 3777400-99 Ext. 2458, Email: waraporn@as.nida.ac.th

## ABSTRACT

E-learning allows us to learn anywhere and usually at anytime convenient to the students. Modern technologies such as computers and the Internet are main infrastructures that enable teachers and students to exchange electronic documentation. To make e-learning successful, however, it is necessary to have the ability not only to exchange electronic documents but also to control such documents after delivery. That is, after a document leaves the teacher's desktop, control is necessary to ensure that the document is only disseminated to his/her intended students. Therefore, this paper presents an environment that is able to track and control all delivered documents, and how to integrate such an environment into e-learning.

**Keywords:** E-learning, Document control, Document tracking.

## INTRODUCTION

E-learning is the electronic or digital delivery of knowledge, information, education and training. It can be CD-ROM-based, network-based, Intranet-based, or Internet-based. It includes text, video, audio, animation, and virtual environments. E-learning allows you to learn anywhere and usually at anytime, as long as you have a properly configured network and computer. It can suffer from many of the same pitfalls as classroom learning, such as boring slides, monotonous speech, and little opportunity for interaction. As in every form of learning, the quality of e-learning is in its content and its delivery [4, 6, 7, 8].

In a typical learning environment, it can be either active or passive, or both. Active learning is the goal-keep learners awake, keep them engaged in their learning, and make them energized participants. That is, one of the requirements of e-learning is the ability to exchange electronic/digital information and documents between a teacher and students. Whenever information or documents leave the teacher or student, control is necessary to ensure that the information or documents are only disseminated to their intended audience. People who write, create, and send information should have the ability to control whatever they send. In lieu of document security, the user loses control of data when he pushes the send button on his email GUI or posts a valuable document on a human resource server.

Thus, this paper presents an environment, which provides access control that stays with documents and data after they are delivered, and how such an environment is incorporated into e-learning.

## MODERN DOCUMENT EXCHANGE

Electronic document exchange is quickly becoming the main way that organizations disseminate information. Email, Word, spreadsheets, and the Web are part of our everyday lives. In this electronic world, nobody thinks twice about zipping up important files with confidential data and sending them from a desktop in the teacher's office to students in the campus.

There is no arguing that the Internet and other technology has made our lives easier, business processes faster, and data more available. But it has also created some new challenges.

In today's work environment a person must be able to send a file with confidence that it won't be intercepted, tampered with, or viewed by someone other than the intended recipient. We all know this is easier to say than to have done. Script kiddies, electronic vandals, and even corporate spies are ubiquitous. Passwords and other confidential information are passed over networks in the clear, and the everyday computer user doesn't think much about security.

There are five different things a systems administrator should consider when trying to create an environment in which a user community can exchange information securely [1, 2, 5, 9].

**Authentication** guarantees that computers, users, or companies accessing documents are who they claim to be

**Access Control** requires users to have the appropriate permission for viewing sensitive data

**Message Integrity** guarantees a document has not been altered

**Accountability** provides an audit trail for tracking electronic transactions

**Revocation** provides a means to dynamically deny access to data at any time without having to recover copies.

Without all five of these elements considered, document exchange can be a company's worst liability.

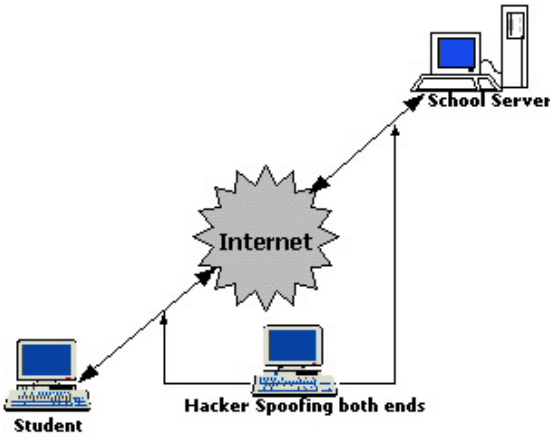
Whether blackhat, whitehat, or greyhat, hackers are a legitimate concern when talking about document control and privacy. They find ways to put themselves in the middle of a transmission being conducted by two other parties, who believe their connection, is secure. They find ways to steal passwords and bring down websites. Hackers also do some good. They find vulnerabilities in software, report weaknesses to the technology community in general, and post information about how to fix the vulnerabilities they expose.

In large part, information transmitted across networks, including the Internet, is transmitted "in the clear." For example, Internet e-mail flows in plain text from the teacher, through one or more Internet gateways, to the student.

Sending e-mail over the Internet can be likened to sending a postcard in the snail mail system. Neither the electronic nor the paper version is in an envelope and many employees and contractors will handle it as it travels to its destination. Any of the handlers can read the email or postcard and it may even get lost.

On the Internet, people who make it their business to hack networks and computers have tools readily available to help them. Network sniffers can be used both for good (network administration functions) and evil (stealing information). Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted al-

*Figure 1: A Simple Example of the Man-In-The-Middle Attack*




most anywhere on a network.

In addition to readily available tools, hackers have figured out how to shim themselves between the route of a two-way communication. In a Man in the Middle Attack, as shown in Figure 1, a hacker places his system between that of a sender and receiver. By spoofing both ends of the communication, a hacker can monitor all the traffic between the endpoints. Admittedly, this is a complex task. But once a hacker successfully executes the attack, he can put the exploit on the Internet for all kinds of script kiddies to download and deploy.

This becomes a scary scenario when we talk about the world of on-line confidential document exchange. What if a hacker successfully planted himself between a home-computer-user doing on-line document exchange? The user sends passwords, account numbers, and confidential information across a wire assuming that he is talking to the school, when his confidential information might be making an intermediary stop at the Dark Lord's computer.

The Man-in-the-Middle attack exploits two problems that must be solved when implementing a good all around security program:

**File Interception** . Interception and alteration of transmitted data by people other than the data's intended recipient

**Authentication**. Ensuring a person or computer system is, in fact, whom you intended or want to communicate with

## PERSISTENT DOCUMENT CONTROL

As now discussed ad-nauseum, file level protection is as important as network level security. After a file leaves the teacher's desktop, control is necessary to ensure that the information is only disseminated to its intended students.

People who write, create, and send all that data inside those zip files, emails, marketing.html, and exam.docs should have the ability to control whatever they send. In lieu of document security, the user loses control of data when he pushes the send button on his email GUI or posts a valuable document on a human resource server.

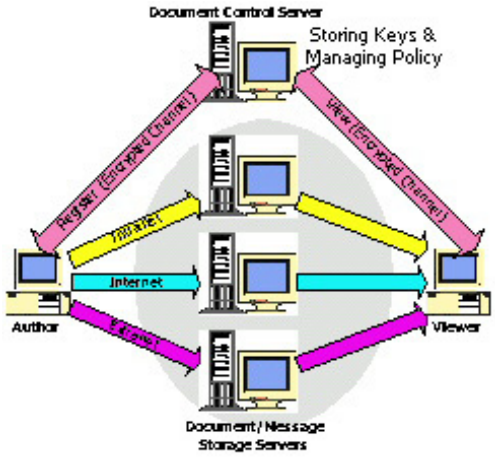
Maybe an organization sells information like lead sheets that they do not want freely distributed. Or maybe another organization inside the same company needs to keep information protected for private or legal reasons. Consequently, there is a strong need for a software environment that will help schools get control over the way important data is stored and distributed.

## A DOCUMENT CONTROL ENVIRONMENT

As shown in Figure 2, the computer software system [3] consists of three main components: a Document Control Server (DCS), Author, and Viewer. These software components combine encryption, authentication, and authorization to protect important information while at the same time allowing the free exchange of ideas and data.

This system can be used in a variety of ways to secure confidential, copyrighted, or secure information while at the same time allowing users the access they need to get their job done. It provides access control that stays with documents and data after they are delivered. After information leaves the complex

*Figure 2: Major Software Components in a Document Control Environment*




world of TCP/IP, routers, switches, NICs, and port allocations, security must be applied on the ends where users are accessing it. If you are concerned about keeping information private and controlling who has access to important data, this system can help.

The system gives document authors total control over who has access to *what* data and *when*. For example, a document that contains the subject testing information might be divided into two sections: *questions* and *answers*. The document's author, the teacher, might want only students, who take this subject, to view the test questions before a specific date, and to be able to see the answers after such date. Under this system, the teacher is able to track who perform the test and when it has been done. In addition, the teacher has the ability to allow students to read the documents, and to prevent them from copying, pasting or forwarding the documents.

## INCORPORATING THE ENVIRONMENT INTO E-LEARNING

After the teacher has finished editing electronic documents that he/she wants to control, he/she has to register the documents to the Document Control Server (DCS), as shown in Figure 2. Then, DCS generates keys used to encrypt the documents and stores the keys in itself (DCS) to decrypt such documents later. Only authenticated students with the proper rights are allowed to access DCS and the keys.

In the registration process, the teacher has to define a policy for controlling the document before delivering to students. In fact, a policy is a set of permissions that defines

- *who* can access a protected document,
- the network entities (i.e. IP address) from *where* they can access it,
- the date and times where they are allowed to access it, and
- activities such as read, print, copy and paste that are allowed to perform while accessing the document.

Before a student can view the protected document, he/she needs to connect to the Document Control Server (DCS) for proving his/her identity. After being authenticated, the student will be authorized access to keys that encrypt/decrypt specific documents. In general, this system can be used with any applications such as email and Web.

## CONCLUSIONS

It has been widely accepted that almost all sensitive information is now in electronic form, and commonly stored in a network-based server. Naturally, once access is granted, information can be copied and distributed anywhere. In other words, authors lose control of their information after transmission. Unprotected documents can be forwarded, copied, printed or modified by any number of people.

In this paper, therefore, we proposed a document control environment mainly based on cryptography technologies. This enables teachers and students to track and control any academic documents after delivery. This environment consists of three main components: a Document Control Server (DCS), Author and Viewer. It can be simply integrated into any e-learning system.

## REFERENCES

[1] C. Adams, and S. Lloyd (1999), Understanding Public-Key Infrastructure : Concepts, Standards, and Deployment Considerations, Macmillan Technical Publishing.

[2] E.G. Amoroso (1994), Fundamentals of Computer Security Technology, Prentice-Hall International, Inc.

[3] Authentica, Inc. (1999), PageVault Server, Available in:http://www.authentica.com.

[4] Lesley S.J. Farmer (2002), Seven Ways to BlackBoard, in 68th IFLA Council and General Conference, August 18-24, 2002.

[5] W. Ford and M.S. Baum (2001), Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Prentice-Hall International, Inc.

[6] Duncan Lennox (2001), Managing Knowledge with Learning Objects – The Role of an E-Learning Content Management System in Speeding Time to Performance, Available in:http://www.wbtsystems.com, Access: September 28, 2002.

[7] M.K. Pinheiro, J.V. de Lima, N. Edelweiss, N. Layaida, and T. Lemlouma (2000), An Open E-Learning Authoring Environment.

[8] J.S.R. Subrahmanyam (2000), Future Trends of Content Management Systems (CMS) for E-Learning: A Tool Based Database Oriented Approach.

[9] W. Stallings (1999), Cryptography and Network Security : Principles and Practice, 2nd Edition, Prentice-Hall, Inc.