Towards a Secure Copyright Protection Infrastructure for e-Education Material: Principles Learned from Experience*

Joe Cho-Ki Yau[1], Lucas Chi-Kwong Hui[1], Siu-Ming Yiu[1] and Bruce Siu-Nang Cheung[2]
(Corresponding author: Joe Cho-Ki Yau)

Department of Computer Science, The University of Hong Kong[1]
Pokfulam Road, Hong Kong. (Email: jckyau, hui, smyiu@cs.hku.hk)
School of Professional and Continuing Education, The University of Hong Kong[2]
Pokfulam Road, Hong Kong. (Email: bruce@hkuspace.hku.hk)

(Received July 7, 2005; revised and accepted Aug. 9, 2005)

Abstract

Copyright of e-Education material is valuable. The need for protecting it is prominent. In the past two years, we have developed an infrastructure called *e-Course eXchange* (*eCX*) for protecting the copyrights of e-Courses, right from its development phase to its delivery phase. It has been adopted by an education institute, with a user-base of over 70,000 students, and has been receiving positive feedback from students. To design a secure and effective copyright protection infrastructure is not trivial. In particular, for efficiency purpose, one may allow students to retain a local copy of the e-Course material in their own computers; on the other hand, we should make it difficult for them to make illegal copies of the material. Only storing the material in encrypted form is not enough to protect the material. In this paper, we summarize some principles and knowledge we have gained through this project that should be observed for designing a secure copyright protection system. We believe that these principles would be useful to developers and researchers for designing and developing such a system.

Keywords: Copyright protection, software protection, reverse engineering, e-Education, e-Learning

1 Introduction

With the advent of the digital age, e-Education has become one of the most important channels for students to acquire knowledge. Students of different levels are one way or the other making use of this new channel to learn, and researchers are actively working on this area to make the best use of it. However, as pointed out by Furnell [9, 10], little attention has been devoted to the security concerns of e-Education. Among these security concerns, the copyright protection problem for the e-Education material is one of the most important concerns that are vital to the operation of e-Education institutes.

Almost in all e-Business sectors, the intellectual property of material or content could be the most valuable asset of the business itself, and this is undoubtedly true for the e-Education sector. Many organizations rely on the income generated from students studying e-Courses. Registered students infringing the copyrights of the course materials by passing the materials to non-registered students can severely jeopardize the income of the organization. Hence, copyrights of e-Course materials must be securely protected.

About three years ago, we initiated a study of the problem of protecting the copyrights of e-Education materials. We proposed an infrastructure, called *e-Course eXchange - eCX* [26, 27, 28, 29]. This infrastructure has been developed and deployed to a large group of users. In this paper, we will use eCX as a case study, and discuss the lessons we have learned from it. In Sections 2 and 3, we will take a closer look at e-Education, its security concerns, and, in particular, its domain specific requirements for copyright protection. In Section 4, we will give a brief survey on the existing copyright protection solutions. In Section 5, we will present the design of eCX. In Section 6, we will discuss the issues and design principles we learned from our experience with eCX. Section 7 then concludes the paper. Although eCX may seem to be a solution specific to the e-Education segment, the lessons we have learned are general enough and applicable to other copyright protection systems.

*This paper represents the personal opinion of the authors and does not represent the official standpoint of HKU SPACE.

2 Background

As e-Education is gaining its popularity, it is also gaining the attention from the research community. Even though the research on e-Education is active, the research on the e-Education related security issues has been studied little. There are quite a number of security concerns in e-Education systems, for example, user authentication and access control, non-repudiation for critical actions, such as course registration, course tuition fee payment, confidentiality of user personal information, course material copyright protection, *etc.* The paper presented by Yang et al. [25] discusses about privacy protection in an e-Education system, while the paper by Furnell *et al.* [9] has given a security framework for e-Education systems. The papers by Cheung *et al.* [4, 5] propose a viable solution to solve the problem of user authentication and access control. In particular, [4] provides a security model such that registered student cannot easily share the account with non-registered students.

Although copyright protection is an active research, the problem of protecting the copyright of e-Course material has not been studied that much. Only Furnell *et al.* [10] briefly studied this problem. However, it does not provide an effective approach for copyright protection and copyright detection in the domain of e-Education. In 2001, a study on protecting the copyrights of e-Course material was initiated by the SPACE Online Universal Learning (SOUL) Project Group of the School of Professional and Continuing Education of the University of Hong Kong (HKU SPACE), one of the leading adult education providers in Hong Kong[1]. This study gives birth to an infrastructure, called *e-Course eXchange - eCX*. It has been designed, developed and deployed to a large group of students, and has been receiving positive feedback from them.

In this paper, we will present our experience and share with readers the lessons we have learned from developing a copyright protection solution for the e-Education sector. In fact, some of the lessons we have learned from eCX could also be treated as general guidelines for the design of copyright protection systems.

3 Particularities of e-Course Delivery

After some research on the accessing pattern and behavior of students participating in e-Education (particularly for students in some parts of the world, such as Mainland China), we discovered that (1) they are not always connected to the Internet; (2) many Internet providers are charging their users based on connection time (in another words, it would be best to minimize students' Internet connection time to save money); and (3) not all of the students enjoy high bandwidth connections to the Internet and accessing bandwidth demanding materials (*e.g.*, multimedia material like audio or video clips) would not be feasible for these students. It is, therefore, an advantage for an e-Education system to allow its students to download the e-Course material onto their own computers and view the material offline. This will allow students to study the material anytime, anywhere, even when they are not connected to the Internet. It is for the same reason that students are relieved from the financial burden of Internet connection time. In the case where the material of the e-Course requires high bandwidth, since the material is already downloaded to students' computers, the connection bandwidth problem will not hinder students from studying.

Even though this notion of allowing students to download e-Course material may seem attractive, it gives great worries to copyright owners of the materials. Caution must be taken to stop users from making illegal copies of the downloaded materials. We need a copyright protection system. In light of this, eCX was designed to address this particular concern.

4 Existing Copyright Protection Systems

As people's awareness on intellectual property rights increases, more and more solutions for protecting copyrights become available in the market. However, most of these solutions are domain specific, and may not meet the needs of the e-Education domain. For example, many of the *eBook* solutions [18, 19, 20] support only text-based materials, offering limited support for graphics, and even less support for audio and video materials, and are not sufficient for e-Education. More importantly, most eBooks solutions are tightly coupled with physical, dedicated electronic book appliances, making them very restrictive and not commercially viable.

On the other hand, major computer technology vendors (*e.g.*, IBM, Intel, Matsushita, Toshiba, and Hitachi) have been joining hands, forming alliances to foster solutions to the problem (*e.g.*, the 4C Entity [1], and the 5C Entity [2]). Solutions that they have proposed are mostly for the storage and the transmission of valuable material. An example for secure storage is *Content Protection for Pre-Recordable/Recordable Media (CPPM/CPRM)* [3], and another example for secure transmission is *Digital Transmission Content Protection (DTCP)* [15]. On the other hand, the system, *eXtensible Content Protection (xCP)* proposed by IBM [12], is primarily used for protecting entertainment content. It aims at providing a way to enable unfettered "domestic" fair use by grouping networked domestic devices into a single DRM domain.

Although we have that many solutions available, they all tend to serve contents of specific domains. As many of the e-Course materials are presented via some web-

[1] HKU SPACE was estimated to have more than 70,000 registered students as of 2004.

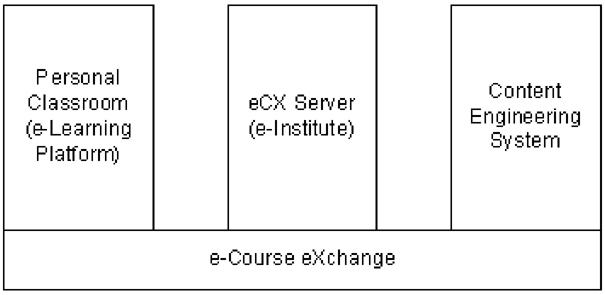
Personal Classroom (e-Learning Platform)
eCX Server (e-Institute)
Content Engineering System
e-Course eXchange

Figure 1: An overview of the SOUL platform

enabled technologies, we find these copy protection solutions insufficient. It is crucial to protect web-delivered materials, and the quest for such a solution is imminent.

5 Our Copyright Protection Infrastructure - eCX

Regarding the system design of eCX, a number of papers have been published, describing its design details. Interested readers please refer to [26, 27, 28, 29]. In this section, we will give a brief overview of its design to facilitate our discussion in the next section.

5.1 The SOUL Platform

eCX is an infrastructure designed for the delivery of e-Courses. It is integrated into the SOUL Platform [21], which is designed to support three different types of e-Education participants: (1) e-Course authors, (2) e-Education providers (*e.g.*, HKU SPACE), and (3) students taking e-Courses. Figure 1 depicts an overview of the platform.

The SOUL Platform is composed of three software suites, and eCX is integrated into these software suites to protect the copyrights of e-Course material. The three software suites are as follows:

- ***Content Engineering System***: The *Content Engineering System* is a software suite used by e-Course authors (namely, teachers and instructors) for e-Course authoring. It assists e-Course authors in publishing e-Courses that they have finished creating to an affiliated eCX Server.

- ***eCX Server***: The *eCX Server* (also known as *e-Institute*) is a server-software, used by e-Education providers for hosting e-Courses for students to download.

- ***Personal Classroom***: The *Personal Classroom* (also known as *e-Learning Platform*) is a software suite that assists users in downloading and viewing the material of downloaded e-Courses.

The eCX infrastructure is designed to protect the copyright of e-Course material. It plays the role of *copy protection* to protect the material in the following 3 areas:

(i) when the e-Course is being transmitted between the three software suites.

(ii) when the e-Course is stored in the computer of the e-Education participants, and

(iii) when the e-Education participants access the e-Courses that are stored on their own computers.

Under the design of eCX, an e-Course could be transmitted from its author to an eCX Server, or from the eCX Server to the students. In both cases, there are specially designed protocol for these transmissions, which make use of Public Key Infrastructure (PKI) and other cryptographic technologies (*e.g.*, *Secure Sockets Layer - SSL*). For details about these protocols, please refer to [29].

Please note that eCX does not protect e-Courses when they are stored in their authors' computers because they are the copyright owners of the e-Courses. That is, eCX will provide protection to e-Course material only when the e-Course is under the custody of e-Education providers or the students.

For the protection of the material when it is under the custody of e-Education providers, it is a typical problem of tightening the security of servers on the Internet. Measures like firewall, closing unused ports, disabling unused services, frequent OS patches, *etc.* should all be applied. For the rest of this paper, we will focus on protecting the material that is under students' custody, and give a security analysis in this area.

5.2 What is an e-Course?

We have been loosely using the term *e-Course* to refer to "*electronic courseware*". But what exactly is an e-Course in the context of eCX? An e-Course in the eCX context is any material that can be delivered via the web. In another words, all materials that can be viewed using a web browser can be used as materials for an e-Course. This includes material of different media types (*e.g.*, text, image, audio and video clips) and web-enabled presentations that involve browser plugins (*e.g.*, Flash, Authorware, Java Applets, *etc.*). There could be many files to an e-Course. The only requirement is that all materials to an e-Course should be self-contained. Also, the files to an e-Course should all reside within a single directory tree. In Section 5.3.1, details about how an e-Course is packaged will be given.

Most e-Course materials we have listed in the previous paragraph are static material. In addition to these static materials, eCX e-Courses are also supported by an intelligent tutoring system (ITS), called *SmartTutor* [6, 30]. SmartTutor provides interactivity to students when students are viewing the course material. It also provides guidance to students, imitating a human tutor, assisting students in their learning activities.

5.3 Personal Classroom

The Personal Classroom is a software suite used by the students. It provides two functions to students: (1) downloading e-Courses, and (2) viewing e-Courses. Also, there are two key technologies in Personal Classroom: (1) *Offline-online Course*, and (2) *Hardware Profile*. In this section, we will explain about these functions and key technologies.

5.3.1 Offline-online Course

In the context of eCX, e-Courses are given a special name: "*Offline-online Course*". This is because an e-Course, which is often referred as "*online course*", is downloaded and viewed by students *offline*. An Offline-online Course is composed of two objects: *Course Package* and *Course Voucher*. The Course Package is a package that contains all of the files in an e-Course. Files in this package are symmetrically encrypted. To access the e-Course material in a Course Package, student must possess the package's decryption key. The decryption key is stored in the Course Voucher. Therefore, a student must possess both the Course Package and the Course Voucher in order to access the material in the e-Course. Please refer to for [29] details of Offline-online Course.

5.3.2 Hardware Profile

At the time of installation of the Personal Classroom, a snapshot of the configuration of the student's computer is taken for creating a *Hardware Profile*. This Hardware Profile is stored in the *Computer License*, and is checked against whenever the Personal Classroom is invoked. The Personal Classroom will continue with its invocation only if the Hardware Profile is successfully verified (that is, it is invoked on the computer where it is originally installed). By using the Hardware Profile mechanism, we can prohibit adversaries from making illegal copies of e-Course by making replication of the student's hard-disk and install the replica onto another computer.

The Hardware Profile is stored in the Computer License of the student's computer. The Computer License is a digital certificate stored in the student's computer. It is issued by the eCX Server that the student affiliates with. It contains various information including student's personal information and the Hardware Profile of the student's computer. Please refer to [29] for details about Computer License.

5.3.3 Downloading e-Courses

The *Downloader* is a software module of the Personal Classroom used by students to download e-Courses. As shown in Figure 2 , the Downloader connects to the eCX Server via the Internet for downloading e-Courses.

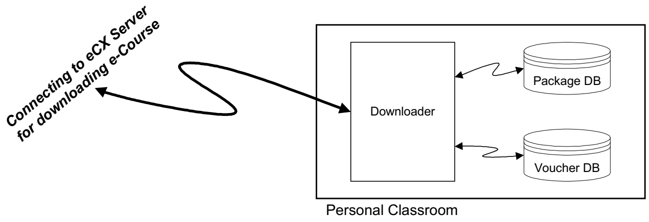

Figure 2: The architecture of the personal classroom - course downloading

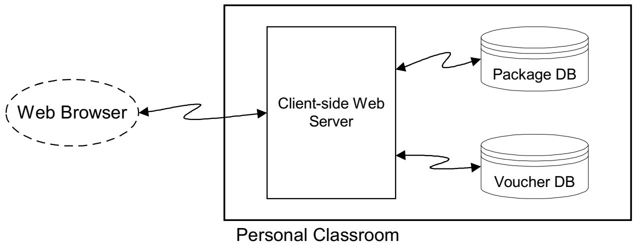

Figure 3: The architecture of the personal classroom - course viewing

For each e-Course that the Downloader downloads, it will obtain both the *Course Package* and the *Course Voucher* of the e-Course. After the Course Package is downloaded, these files will be unpacked and stored in the *Package Database*. Note that all of these files are symmetrically encrypted, and the decryption key is stored in the Course Voucher. All downloaded Course Vouchers are stored in the *Voucher Database*, which is an encrypted database. The decryption key, which is essential for accessing this database, is stored somewhere in the student's computer, hidden from the student.

5.3.4 Viewing e-Courses

Students can make use of the Personal Classroom to view e-Courses that they have downloaded. When a student invokes the Personal Classroom for viewing e-Course, the Hardware Profile will first be verified. Once this verification is successful, the Personal Classroom will continue with its invocation and operate under the *course-viewing mode*, as illustrated in Figure 3.

When Personal Classroom operates in the course-viewing mode, it will invoke a *client-side web server*. This client-side web server is a customized web server that knows how to access files in the Package Database, and retrieve Course Vouchers from the Voucher Database. Since the Course Voucher contains the encryption key for the files of the e-Course, the client-side web server is capable of decrypting the e-Course material. Note that for a student to view the e-Course material, the student has to invoke a web browser to connect to the client-side web server, and browses the material as if the student is accessing the material from an ordinary website.

6 Security of eCX

Since the deployment of the eCX infrastructure in HKU SPACE a few years ago, it has undergone some minor revisions. From a technical point of view, we have observed a few principles on designing copyright protection systems. In this section, we will try to analyze eCX, and list the pitfalls we encountered when implementing this system.

6.1 The Danger of an Un-secure Reader

As described in Section 5.3.4, all of the material of an e-Course is installed on the student's computer and accessed via the Personal Classroom, which makes use of a customized client-side web server running on the student's computer. One possible attack would be for an adversary to make use of a web browser to access the material, and invoke the *save* function of the web browser to obtain copies of the material. Please note that if the content of the e-Course involves many different files, the adversary would only be able to save one web page at a time, and would have to invoke the save function many times in order get a complete copy of all the files of the e-Course. Or, better yet, the adversary can use some command line based web client that is capable of downloading web content recursively (*e.g.*, "wget" [24], which can greatly speed up the process of pirating a copy of the material.

This type of attack to a copyright protection system is quite common, and can defeat the system by making illegal copies of the content. In fact, this attack could be generalized to other copy protection systems. Many copy protection systems protect the material by encrypting it. The system then in turn protects the encryption key itself, which is usually much smaller in size than the material itself. For the case of eCX, the material is packaged and encrypted to become the Course Package, and the encryption key is stored in the Course Voucher itself, which can only be accessed by the Personal Classroom. In other words, we can be certain that the material is securely protected while it is stored in the user's computer. However, when the material is viewed/accessed with some *reader application* (in the case of eCX, it is the web browser), the material must still be carefully protected.

One lesson we can learn from this is that the material must be protected *from end to end*. When a user views the material, it is important that the material should only be viewed with web browsers that are secure (namely, the web browser will protect the copyright of the material). Typically, a copyright protection system should develop its own reader application to access the material.

To solve this problem, eCX was revised. We have built for eCX a *customized web browser*. Certain functions, including saving, printing, copying, and many other functions, are disabled and removed from this customized web browser. Also, we have modified our client-side web server so that it will only serve requests from our customized web browser, and not any other.

A general rule for designing copyright protection systems is for the system to have its own "reader application" for accessing or viewing the protected material. An example of such a "reader application" would be the *Windows Media Player* [13] produced by Microsoft for protecting streamed and downloaded audio and video content. The content is protected all the way from the content hosting server to the application for accessing or manipulating the content.

6.2 Capturing of Localhost Traffic

Besides tightening our security at the "reader application" level, we also find that securing the communication between our customized web browser and our client-side web server to be important. Since we are relying on HTTP for the communication between these two software components, it would be insecure if this communication were not carefully protected. Imagine that if an adversary captures the traffic between these two components, it would be easy for the adversary to reconstruct the original content sent between the two components. There are many tools available on the Internet that can be used for capturing network traffic. In particular, the Ethereal network protocol analyzer [7] is capable of capturing the network traffic and reconstruct the content of the communication.

After some detailed investigation, we discovered that not all operating systems permit the capturing of localhost communication [11, 17]. In particular, the Windows operating systems from Microsoft, target operating systems of our Personal Classroom, do not support the capturing of localhost traffic, and that means we are not vulnerable in this regard. However, the general rule we find for protecting material being transmitted is by using some secure communication protocol (*e.g.*, SSL or HTTPS). Even if the traffic is captured, the adversary would not be able to decrypt the traffic.

6.3 Reverse Engineering

Another possible attack to eCX is by reverse engineering. Typically, crackers would use software hacking tools, such as SoftICE [21] or some low level debugger, whereby the cracker can detect entry points to dynamic link library (dll), make patches to the software, and hence bypassing critical processes like invocation validation. Skillful crackers could also trace the workflow of the software and uncover hidden data (such as decryption keys) from the software. Since Personal Classroom is a software suite that is deployed and executes on students' computers, it imposes threats to the system if crackers can reverse engineer Personal Classroom and illegally make copies of downloaded e-Courses.

There is no single principle to protect software from reverse engineering. In fact, it is another huge research topic. However, one principle we have learned during the development of eCX is that it is important for developers to adhere to principles for the development of secure software [8, 16]. For example, the integrity of important files (*e.g.*, executable files, shared library files, *etc.*) are checked before they are loaded; sensitive information (*e.g.*, checksums or encryption keys) that must be hard-coded are stored in their encrypted form, and are decrypted only when they are in use; security checking functions and validation functions do not just return boolean information, but return data that are to be used somewhere else in the processing of a later stage so that bypassing the validation by simple modification to the programs would not be possible.

There are many more principles and techniques for the development of anti-reverse engineering software. It is a matter of good software development practice, security awareness and experience that cannot be easily confined in a couple of written rules. It is an area that requires the attention of researchers.

6.4 Virtual Machine Attack

Another security threat to eCX is by installing the Personal Classroom onto virtual machines. There are, nowadays, many software for computer virtualization [14, 23]. They could be used for virtualizing a computer system on the host computer, and has its own hardware configuration. This implies that within the virtual machine, the hardware configuration is identical, regardless the configuration of the underlying host computer. This computer virtualization software typically saves the state of the virtual machine in the form of ordinary disk files onto the hard-disk of the host computer. Hence, it is very easy to make a perfect duplication of the virtual machine by just making copies of those disk files.

This notion of computer virtualization poses a problem for eCX. Since the virtual machine has its own hardware configuration, our Hardware Profile mechanism described in Section 5.3.2 may not be effective. Also, it is difficult for a software program to detect if it is running on a virtual machine. If an adversary installs the Personal Classroom in a virtual machine, and downloads e-Courses onto this virtual machine, it is possible for the adversary to redistribute the whole virtual machine to others by just making copies of the disk files of the virtual machine. In general, due to the nature of virtual machines, it creates lots of problems for researchers of copyright protection.

This is in fact a very hard to solve problem. Many people have been looking into the problem of detecting virtual machine execution environment. However, this detection depends on the concerned machine virtualization software, and cannot be easily generalized. But, at the moment, machine virtualization software is still not very popular. Redistributing the Personal Classroom in the form of a virtual machine is a very *expensive and heavy approach*. It requires the person using the pirated copy of eCX to have the machine virtualization software installed, which the virtualization software itself is expensive and cannot be easily comprehended by general or inexperienced computer users. Also, the size of the disk files for a virtual machine is typically in the range of a few gigabytes, which incurs quite an expensive cost for the redistribution of Personal Classroom. However, this type of attack still poses a very dangerous threat to copyright protection systems.

7 Conclusion

In this paper, we study the importance of protecting the copyrights of e-Education material. We also study design concerns that are specific to the e-Education domain. We briefly introduce our solution, called e-Course eXchange (eCX), which allows students to retain a local copy of the e-Course material in their own computer, and yet difficult for making illegal copies of the material. We also analyze the design of eCX, and present a number of principles we have observed during the development of eCX that are important for the design of copyright protection systems in general. In particular, a copyright protection system should provide its own "reader" or application for accessing the protected content. It should also be carefully designed to avoid reverse engineering attacks. We also point out that attacking a copyright protection system by using virtual machines is very difficult to defend, and yet, a very experience and heavy approach for attacking.

eCX has been deployed in HKU SPACE and has been receiving positive comments from instructors and students. However, from a technical point of view, there are yet many areas that worth further studies: how can we better protect our software from reverse engineering? How can we detect if our software is running on a virtual machine? These are interesting problems that worth further research.

Acknowledgements

This research is partly supported by various grants of the Hong Kong Special Administrative Region, China, including the Areas of Excellence Scheme (Project No. AoE/E-01/99), two grants from the Research Grants Council (Project No. HKU/7144/03E and HKU/7136/04E), and two grants from the Innovation and Technology Commission (Project No. ITS/170/01 and UIM/145).

References

[1] 4C Entity, *Welcome to 4C Entity*, http://www.4centity.com/.

[2] 5C Entity, *Welcome to the DTLA*, http://www.dtcp.com/.

[3] 4C Entity, *Content Protection for Recordable Media*, http://www.4centity.com/tech/cprm/.

[4] B. Cheung, L. C. K. Hui, T. Yim, and V. W. L. Yung, "Security design in an online-education project," in

Proceedings of the Fifth Hong Kong Web Symposium on e-Education: Challenges and Opportunities, pp. 1–14, Oct. 4-6, 1999.

[5] B. Cheung and L. C. K. Hui, "Student authentication for a Web-based distance learning system," in *Proceedings of the Fifth International Conference on Information Systems Analysis and Synthesis*, pp. 441–446, July 31 - Aug. 4, 1999.

[6] B. Cheung and L. K. Kwok, "SmartTutor for lifelong learning," in *Proceedings of the 5th International Conference on New Educational Environments*, Lucerne, Switzerland, May 26-28, 2003.

[7] Ethereal, *Web Site of the Ethereal Network Protocol Analyzer*, http://www.ethereal.com/.

[8] Fravia, *FRAVIA'S How to Protect Better*, http://www.searchlores.org/protec/protec.htm.

[9] S. Furnell, P. D. Onions, M. Knahl, P. W. Sanders, U. Bleimann, U. Gojny, and H. F. Röder, "A security framework for online distance learning and training," *Internet Research: Electronic Networking Applications and Policy*, vol. 8, no. 3, pp. 236–242, 1998.

[10] S. Furnell, U. Bleimann, J. Girsang, H. F. Röder, P. Sanders, and I. Stengel, "Security considerations in online distance learning," in *Proceedings of Euromedia 99*, pp. 131–135, Apr. 25-28, 1999.

[11] G. Harris, *Re: [Ethereal-users] Can I capture Internal Communication?* http://www.ethereal.com/lists/ethereal-users/200112/msg00145.html, Dec. 27, 2001.

[12] International Business Machines Corporation, *IBM Response to DVB-CPT Call for Proposals for Content Protection & Copy Management: xCP Cluster Protocol*, http://www.almaden.ibm.com/software/ds/Content Assurance/papers/xCP_DVB.pdf, Oct. 2001.

[13] Microsoft Corporation, *Architecture of DRM*, http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.asp.

[14] Microsoft Corporation, *Microsoft Virtual PC 2004*, http://www.microsoft.com/windowsxp/virtualpc, 2004.

[15] B. Pearson, *Digital Transmission Content Protection*, http://www.dtcp.com/data/dtcp_tut.pdf, June 1999.

[16] F. Piessens, *Developing Secure Software Applications*, http://www.cs.kuleuven.ac.be/∼frank/OVS/Cursus OVS-2004.pdf, Nov. 25, 2004.

[17] M. Regner, *Re: [Ethereal-users] Capturing Localhost/Localhost Traffic on Windows 2000*, http://www.ethereal.com/lists/ethereal-users/200212/msg00166.html, Dec. 22, 2002.

[18] J. hene-Djan, "Personalising electronic books," *Journal of Digital Information*, vol. 3, no. 4, Feb. 2003.

[19] Open eBook Forum, *Welcome to the OeBF*, http://www.openebook.org/.

[20] N. Shiratuddin, M. Landoni, F. Gibb, and S. Hassan, "E-Book technology and its potential applications in distance education," *Journal of Digital Information*, vol. 3, no. 4, Feb. 2003.

[21] SoftICE, *Web Site of SoftICE*, http://www.compuware.com/products/driverstudio/softice.htm.

[22] SOUL, *Web Site of the SOUL project*, http://soul.hkuspace.org.

[23] VMWare Inc., *VMWare is Virtual Infrastructure*, http://www.vmware.com/.

[24] GNU (wget), *GNU wget*, http://www.gnu.org/software/wget/wget.html.

[25] C. Yang, F. O. Lin, and H. Lin, "Policy-based privacy and security management for collaborative E-education systems," in *Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002)*, pp. 501–505, Cancun, Mexico, May 20-22, 2002.

[26] J. C. K. Yau, L. C. K. Hui, B. S. N. Cheung, S. M. Yiu, and J. K. W. Lee, "PowerEdBuilder - A universal secure e-learning infrastructure," in *Conference Proceedings of SSGRR 2002 (Winter) International Conference on Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet (SSRGG 2002w)*, L'Aquila, Italy, Jan. 21-27, 2002.

[27] J. C. K. Yau, L. C. K. Hui, B. S. N. Cheung, and S. M. Yiu, "An online course material copyright protection scheme," in *Conference Proceedings of International Network Conference 2002 (INC2002)*, July 2002, UK.

[28] J. C. K. Yau, L. C. K. Hui, B. S. N. Cheung, S. M. Yiu, and V. L. S. Cheung, "A cryptographic schemes in secure e-course eXchange (eCX) for e-course workflow," in *Conference Proceedings of SSGRR 2002 (Summer) International Conference on Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet (SSRGG 2002s)*, L'Aquila, Italy, July 29 - Aug. 4, 2002.

[29] J. C. K. Yau, B. S. N. Cheung, L. C. K. Hui, and B. S. N. Cheung, "eCX: A secure infrastructure for e-course delivery," *Internet Research: Electronic Networking Applications and Policy*, vol. 13, no. 2, pp. 116–125, 2003.

[30] J. Zhang, B. S. N. Cheung, and B. S. N. Cheung, "An intelligent tutoring system: SmartTutor," in *Conference Proceedings of The World Conference on Educational Multimedia, Hypermedia & Telecommunications (ED-MEDIA 2001)*, pp. 2130–2131, June 25-30, 2001.

Joe Cho-Ki Yau is currently Ph.D. student of the Department of Computer Science, the University of Hong Kong. He received a B.Math (Computer Science) from the University of Waterloo, and a M.Phil from the University of Hong Kong. He is the chief architect for the eCX project, and the leader for the eCX research and development team. His research ares is computer security, particularly in digital rights management, copyright protection, software protection, trustworthy computing, and e-Voting.

Lucas Chi-Kwong Hui is the founder and Honorary Director of the Center for Information Security & Cryptography, and concurrently an associate professor in the Department of Computer Science, The University of Hong Kong. He has published more than seventy research papers in international journals and conferences, and has obtained more than 2.5 million US dollars research grants including several industrial collaboration projects. The technology developed in those project had been used by various government and commercial organizations.

Siu-Ming Yiu received a BSc in Computer Science from the Chinese University of Hong Kong, a MS in Computer and Information Science from Temple University, and a PhD in Computer Science from The University of Hong Kong. He is currently a Teaching Consultant in the Department of Computer Science of the University of Hong Kong. His current research interests include Computer Security, Cryptography, and Computational Biology.

Bruce Siu-Nang Cheung is a Senior Programme Director of the School of Professional And Continuing Education, the University of Hong Kong (HKU SPACE). With 20 years' experience in the education technology and applied artificial intelligence fields, Dr. Cheung has involved in numerous research projects on adult continuing education with the exploit of advanced technology such as artificial intelligence, e-copyright protection and datamining. While specialising in e-learning development, his mastery expands into areas of strategic planning and design, application of technology and pedagogical consultation. He received the Director's Award for Innovation in 2001 and the Outstanding Performance Award in 2002 from HKU SPACE to commend his outstanding contributions in SOUL Project (SPACE Online Universal Learning) since 1998. Besides, Dr. Cheung is the Senior Progamme Director of the School's Information Technology division and is responsible for introducing IT and e-Commerce into HKU SPACE programmes.