IGI PUBLISHING **ITB15139**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, **Strategies and Technologies for Developing Online Computer Labs for Technology-Based Courses** edited by L. Chao © 2008, IGI Global

Chapter VIII

Online Computer Lab Security

Introduction

Before an online computer lab is ready for students to perform hands-on practice, security measures need to be enforced to protect the computer lab and even more importantly to protect the university's network. Since the computer lab is online, it is exposed to hundreds of malicious viruses. Once a computer is infected by viruses, the viruses will damage files, multiply themselves to occupy the memory and hard disk space, or take away the central processing unit (CPU) process power and make the computer run very slowly.

When uploading homework assignments, students may spread certain kinds of viruses through e-mail. During hands-on practice, students may need to download some files from other Web sites; it is possible that they may download some Trojan viruses. When activated, the Trojan virus may delete files on a hard drive or send some sensitive information to others.

If an online computer lab is not properly protected, hackers may be able to log on to its computer systems to change the lab settings, delete system files, or simply use the lab resources for their own purposes. It will be even more serious if hackers access the university's network through the online computer lab. The data owned by some offices such as accounting are much more sensitive than the data used in a computer lab. Sometimes, if the network is not properly configured, even some students may be able to access the sensitive data transferred over the university's network.

In the online computer lab, damages caused by security problems often lead to the shutdown of the entire lab. It will take some time to recover the lab. If the university's network is harmed by a security problem, not only can it cause a huge loss, but it may also trigger the university to shut down the online computer lab permanently. Therefore, the online computer lab needs to be well protected to prevent serious security problems. On the other hand, rigorous security measures may cause some conflicts since students need the administrator's privilege to perform certain hands-on practice. In this chapter, we will deal with some of the security issues and come up with some solutions to the problems.

To make online computer labs secure, the first job is to figure out what to protect. Network managers need to investigate the potential vulnerability in an online computer lab. The results of the investigation should be used as a guideline for security policies developed by a team of network managers, instructors, and university administrators. The security policies should cover the issues related to the availability, reliability, integrity, and confidentiality of the computer systems and networks used by an online computer lab. We will have an overview about security technologies and security measures imposed by these technologies. The last topic to be covered in this chapter will be security management. We will discuss management planning and the tools used to implement the management plan.

Background

Security issues in e-learning are one of the greatest concerns among many higher education institutions (Weippl, 2005). It takes joint effort from university administrators, lab managers, faculty members, and students to keep online computer labs secure. All the people involved in the development of online computer labs should understand how security problems threaten e-learning projects and how to protect e-learning projects from these threats (El-Khatib, Korba, Xu, & Yee, 2003). To successfully run an online computer lab, we must consider the issues such as privacy and security. Policy makers need to fully understand the privacy requirements and security assessment. They also need to understand security technologies for enforcing security measures.