Approaches to Computer Lab Management: Lockdown vs. Freedom

Christopher Jones
University of Oregon
Eugene, Oregon 97403
541-346-2094
jonesey@darkwing.uoregon.edu

Yasemin Tunc
Ball State University
University Computer Labs
Muncie IN 47304
ytunc@bsu.edu

Deborah Cherry
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213
412-268-8171
dc30+@andrew.cmu.edu

ABSTRACT
Basic approaches to computer lab management range along a spectrum from total lockdown of lab computers to total freedom. Total lockdown, which can be implemented with system permissions and policies as well as software such as FoolProof and OnGuard, usually means that the computers' storage devices, especially the hard drives, are restricted, preventing write access by lab users (temporary drive space is sometimes available). Lab users are not allowed to install programs or save files and need to go through official channels to have their programs installed. This approach is intended to minimize support issues, protect software licenses and protect the institution from unauthorized software use.

The total freedom approach allows users to use the lab computer as if it were their own. The lab manager then uses a tool such as PC-Rdist, Ghost, or Assimilator to return the computer to a clean state. This can be done at regular intervals (once a day, once a week etc.), at every startup, or on an as-needed basis. In some cases, users themselves can refresh a lab computer. This approach is intended to allow students flexibility and unlimited access to the computer. Drawbacks include inconsistent computers in the labs (especially between rebuilds) and increased network usage during the rebuilding procedure.

This panel will discuss both approaches from technical as well as managerial perspectives. Panelists will represent approaches ranging across the spectrum of management strategies between lockdown and freedom. The panel discussion should be helpful for attendees who support computer labs or provide desktop support.

Keywords
Computer labs, clusters, Ghost, Assimilator, PC-Rdist, RevRdist, KeyServer, student.

1 ABOUT COMPUTER LAB MANAGEMENT

LEAVE THIS TEXT BOX IN PLACE AND BLANK
software license-sharing product, is not primarily a security product, but it can provide an additional layer of protection from intellectual property piracy in your labs.

On Windows operating systems, Registry and Policy Editors are often used to set permissions for certain actions. The multiple user architecture of Windows NT and Windows 2000 provide additional security options, allowing administrators to apply security settings to individual files and users, or to groups of users. Additional commercial software can be installed to further restrict the ability of students to install or modify software, delete or save files, or change system settings.

On Mac OS computers, Mac OS 9 offers some protection with its multiple users feature, which is the Mac OS's first real attempt at building in some protection of the operating system from its users. The multiple users features are fairly easy to circumvent, however, so locking down the Mac OS in an effective manner requires commercial software.

UNIX computers, with their long history of multiple-user operating systems, are usually set up in a restrictive manner by default. Regular users, though they may be able to do quite a bit in their own home directories, are almost never permitted to install software to system directories or modify system settings.

The lockdown approach is intended to minimize support issues, protect software licenses and protect the institution from unauthorized software use. Since users are forbidden to make significant changes to the system, maintenance requirements are generally minimal. The primary drawback of the lockdown approach is its potential to frustrate students who, in order to accomplish an academic task, need to do something to the computer that they are prevented from doing. The lockdown process may make it difficult, time-consuming, or both for managers to install or upgrade software unless the security system is combined with a software distribution mechanism that can cooperate with the lockdown system.

3 THE FREEDOM APPROACH
The freedom approach allows users to use the lab computer as if it were their own. No restrictions are placed on the user's ability to install software, make changes to the system, or save files. This approach is intended to allow students flexibility and unlimited access to the computer. If students need to install software in order to accomplish an academic task or make their computing lives easier, they are free to do so.

The primary drawback to this approach is that students may inadvertently or intentionally disable some of the functionality of the computer. When this happens, the lab manager or the student needs to have a way to return the computer to a clean, functional state.

Software tools such as PC-Rdist, RevRdist, Ghost, or Assimilator can return the computer to a clean state. This can be done at regular intervals (once a day, a week etc.), at every startup, or on an as-needed basis. In some cases, users themselves can refresh a lab computer. The tools in this category are of two types: one type wipes out the whole disk and replaces it with a fresh copy, while the other type compares each file on the disk with a reference set of files, downloading or deleting individual files as needed. Ghost, from Symantec, makes an image of an entire disk or partition. When a restore is needed, the lab manager wipes out the disk or partition by reloading the disk image over the existing disk. While not very elegant, this type of restoration is quite effective. Assimilator, a Mac OS program from Stairways, along with the similar RevRdist (for Mac OS) and PC-Rdist (for Windows), compare files on a disk to a corresponding set of files on a networked volume or CD. Files that do not belong are deleted, and files that have changed are replaced with fresh copies. Sensitive files can be marked on the reference volume so that they are downloaded only in certain situations, or not at all. Students can often run the restore procedure themselves; if significant changes have not been made, it takes just a few minutes to clean up the computer and reboot.

With either type of tool, it is easy to maintain a folder, disk, or partition that remains untouched by the restoration tool. This way, students can have a safe haven for their temporary files even if the operating system and applications need to be completely wiped out and restored.

Drawbacks to the freedom approach include inconsistent or poorly functioning computers in the labs, especially between restores, and increased network usage during the restoration procedure, as well as down time on individual computers while they are being restored.

4 ALTERNATIVE APPROACHES
The most common approach, given the drawbacks of the two approaches outlined above, is some combination of lockdown and freedom. Lab users are often prevented from making drastic changes to the system, just as they are prevented by physical security from walking away with the computers. The most secure lockdown approach can leave the computer virtually unusable without constant intervention by the lab manager to temporarily override restrictions. Many lab managers, especially those with hundreds of computers and small staffs, use a program such as Ghost or Assimilator to restore computers to a base state, but employ various lockdown methods to reduce the frequency, duration, or both of needed restores.

An approach not often discussed but employed more frequently than we like to admit is the "laissez-faire cross-your-fingers" approach, in which a lab is deployed with no restrictions on what students can do to the computers and no easy way of restoring the computers to their original states. Managers who maintain busy labs using this approach spend a lot of time troubleshooting problems and reinstalling operating systems and applications. In very simple situations, such as old computers used as web/e-mail kiosks, this approach may be adequate; a quick perusal of the hard drive and a trip to the Add/Remove Software control panel once a week may be enough to keep such a computer working fine for months, or even the whole academic year.

5 APPLICATIONS TO DESKTOP COMPUTING SUPPORT
Lab management tools are not just for lab managers anymore, as any Symantec salesman would be happy to tell you. Many of us who support individual computer users, usually faculty and staff, and their desktop computers, find that lab management software can be employed in managing individual desktop computers as well. Administrative staff, especially, tend to require a standard set of applications; a two-partition hard drive with the operating system and applications on one partition and personal work files...
on the other partition is not very different from a lab computer with a partition for the system and a partition for the students' work. If staff can be educated to store their files on the second drive, the primary partition can be wiped out and restored with minimal negative effects on the staff members' work.

6 WHICH APPROACH WILL WORK FOR YOU?
The approach you take to managing your computer labs will primarily depend on the needs of your customers, your resources, and the technical inclination of you and your staff. You may also find guidance, limitations, or both in your institution's official technology guidelines. You will no doubt find yourself striking a balance that is appropriate for your environment.

7 FURTHER INFORMATION ABOUT SOFTWARE PRODUCTS MENTIONED IN THE PANEL

7.1 Mac OS Software
Hi-Resolution, makers of MacAdministrator & MacPrefect: http://www.hi-resolution.com/
RevRDist: http://www.purdue.edu/revrdist/
Assimilator: http://www.stairways.com/assimilator

Apple Mac Manager:
http://www.apple.com/education/k12/networking/differ/index.html#macmanager

Apple Network Assistant:
http://www.apple.com/education/k12/networking/appleshareip/ana/

Apple Software Restore:

7.2 Windows software
Symantec, makers of Norton Ghost: http://www.symantec.com/
Pyzzo, makers of PC-RDist: http://www.pyzzo.com/
NT Package (developed at CMU):
http://dist.andrew.ad.cmu.edu/clusters/package

7.3 Cross-platform software (Windows and Mac OS)
PowerOn Software, makers of OnGuard:
http://www.poweronsw.com/
SmartStuff Software, makers of FoolProof, LabExpert:
http://www.smartstuff.com/
Sassafras Software, makers of KeyServer:
http://www.sassafras.com/