Securing Microsoft Windows® for On-line Testing

Dr. Fred Weber

Department of Chemical Engineering
The University of Tennessee

Abstract

Beginning in fall of 2002 the Chemical Engineering department at The University of Tennessee required all sophomores to bring a laptop computer to class. One use of the computer was on-line testing in the classroom. This paper focuses on techniques for securing the windows operating system (NT or later) for on-line assessment.

Criteria for the project included:

- As secure as traditional paper and pencil testing
- No additional applications installed on the student's computer
- Inexpensive
- Easy to implement

The solution consisted of having students login to a Windows domain server. During the logon process, the student's computer is configured to only allow access to selected laptop and web resources during the assessment. There is no additional cost involved if a Windows domain server is available. Finally, this system is easy to implement.

Introduction

Beginning in Fall 2002, all sophomores were required to bring a laptop computer to their chemical engineering classes. One of the first applications of laptops in the classroom was on-line assessment. There are many pedagogical advantages to using on-line assessments in class. For example, students receive immediate feedback on the exam. They not only see their grade as soon as they finish the exam, but with a properly designed assessment, they also have feedback on what they did wrong on a given problem. Although it requires more time to develop an on-line assessment, the instructor does not need to grade it.

Current on-line assessment systems only allow for multiple-choice, true/false, fill in the blank, and similar types of questions. Many engineering educators argue that these types of questions are not appropriate for engineering education since they are unable to grade a numerical answer to an acceptable range. One application where existing tools are adequate is assessing student mastery of a concept.[1] For this type of assessment, the instructor and students get immediate feedback on whether or not the material has been mastered. It is important to secure the testing environment in this application so that the instructor can trust the results. In addition, the author is developing an on-line testing system that will be able to grade an answer to a range of acceptable answers. Thus there is a need for a secure on-line testing environment.

The only drawback to on-line assessment is the many new ways students can cheat. As stated by Neil Rowe, "From a practical standpoint, it is often easier to cheat online (since what or who the assessee brings to the assessment cannot be seen), which increases temptation."[2]

New ways students can cheat include:

- Using the computer to e-mail each other in the class or perhaps someone outside of class who has already completed the course,
- Using instant messaging to communicate with others,
- Visiting other websites to look up information to help with the assessment,
- Assemble extensive "cheat sheets" in electronic form on their computer and use them during the assessment,
- Use various software tools to solve problems that the instructor might not want to allow on the assessment.

The root problem is that students now have a fully functional computer at their fingertips during the assessment. It is necessary to prevent unauthorized use of computer resources without preventing the assessment from working. A secure on-line assessment system is necessary to achieve this goal. To this end, criteria were chosen to guide the development of a secure on-line assessment environment. This system should:

- Be as secure as traditional paper and pencil testing,
- Not require additional applications on the student's computer,
- Be inexpensive, and
- Be easy to implement.

Various techniques were studied to prevent these new cheating techniques. One method that was investigated was to completely block access to the campus network in the classroom. This required access to the physical network, which most schools will not permit. In addition, a separate network and server would have to be supplied in the room to support the online assessment. Another method considered was a "packet sniffer" that can monitor what students are doing on the web. This type of solution was found to be too complicated for most instructors to handle.

Commercial products[3,4] exist to create a secure on-line testing environment but they are expensive and require preloading of software on the student's computers. These were rejected based on these two problems.

The final solution involved using features of the Windows operating system and server technology to secure the computer. Three different features of the Windows environment were used: policies, profiles, and the content advisor in Internet Explorer. Details of each of these are discussed in the following sections. When students login to the Windows domain server, their computer is automatically secured and ready for the on-line assessment.

Controlling Access to System Resources with Policies

Windows policies[5] are used to automatically apply registry settings to a users computer during login. Most of the policies set by the secure on-line assessment system are related to restricting access to system resources.

Windows servers have an easy to use graphical user interface (GUI) for setting these policies. The actual name of the program depends on the “flavor of the server” but they all function in a similar manner. Policies are grouped into similar types and a typical “tree” menu is used to access each policy.

All policies have three possible settings, “checked”, “clear”, and “grey”. It is important to differentiate between these settings. Checked means to apply the policy, clear means to **not** apply the policy, and Grey means don’t affect the current setting on the computer. All these settings must be set to checked or clear to make sure that the security is enforced. In addition, it is important that the policy be read very carefully since some are written in a positive way while others in a negative manner.

A detailed discussion of the policy settings to secure a student’s computer is given below. Related policies are grouped together. The first item is the group name for the policy. The section item (if any) after the “/” is a subgroup of the group name. The rest of the lines detail the individual policy settings. Some of these settings give a second tier of security. Other settings provide the primary security but if a student should find a way around that setting, these others serve as a backup. In the following discussion, only those policies that should be checked are listed. Any others in a group should be unchecked.

Shell/Restrictions
- Remove Run command from start menu √
  - This eliminates access to the dos prompt and other programs through the command window.
- Remove folders from Settings on Start menu √
- Remove Taskbar from Settings on Start menu √
  - The previous two policies remove the settings menu from the start menu. This eliminates access to the control panels and printers and networks
- Remove Find command from Start Menu √
  - This prevents students from using the Find command to execute programs.
- Hide drives in My Computer √
- Hide network neighborhood √
- No Entire Network in network neighborhood √
- No workgroup contents in network neighborhood √
- Hide all items on desktop √
  - The previous five policies prevent access to programs, shortcuts and other resources on their desktop
- Don’t save settings at exit √
  - This prevents students from changing the settings in the secure profile and changing the security level on next login

System/restrictions

- Disable Registry editing tools √
  - This prevents students from editing the registry and unlocking the secure environment. Since the security is created by setting registry settings these must be blocked.
- Run only allowed Windows applications √
  - This guarantees that students cannot run any programs other than what the instructor wishes. If access to a program is necessary, the instructor can add it to a list of allowed programs associated with this policy. Since students cannot get to any programs directly, the best way for students to have access to a program is for the instructor to put a link on the assessment web page that downloads a document for that application. This starts the software and students can then control tab between the running programs.

Windows NT Shell/Custom Shell

- Custom Shell √
  - This policy has an edit field to set the replacement for the usual Windows desktop program to "c:\Program Files\Internet Explorer\IEXPLORE.EXE". This is the most important setting. This replaces the normal Windows desktop with Internet Explorer. The desktop is completely blank except for the Explorer windows. If the student quits explorer, they only have a blue screen. This is not the infamous "blue screen of death" but is only a blank screen. Since the taskbar and start menu are a part of the desktop, they also in unavailable.

Windows NT Shell/Restrictions

- Remove View->Options menu from Explorer √
  - This helps prevent mischief from students by blocking some important commands in Internet Explorer.
- Remove Tools->Go To menu from Explorer √
  - This also helps prevent mischief from students by blocking important commands in Internet Explorer.
- Remove File menu from Explorer √
  - This helps prevent mischief from students by blocking important commands in Internet Explorer.
- Remove common program groups from Start menu √
  - This helps prevent access to programs if other techniques are breached.
- Disable context menus for the taskbar √
  - This helps prevent access to the task manager.
- Disable Explorer's default context menu √
  - This helps prevent mischief from the students by blocking some important commands in Internet Explorer.
- Remove "Map Network Drive" and "Disconnect Network Drive" √
  - This helps prevent students from connecting to other network drives.

Windows NT System

Disable Task manager √

Students can do serious probing of current state of the computer with the task manager, so it needs to be blocked.

Disable Change Password √

This prevents students from changing the logon password to the secure on-line assessment system. Since one logon account is shared by all users this cannot be allowed.

In addition to setting policies for the login account as defined above, it is important to also set policies related to the use of policies themselves and a few other items. This is done in a different policy file on the server called “Default Computer ”.

Network/System policies update

Remote update √

This ensures that the student cannot block the entire policy system. This setting forces the student’s computer to download and apply the policies during the login process.

Logon

Do not display last logged on user name √

This prevents the logon name of the secure on-line testing system from appearing the next time the student logs on to their computer.

Windows NT User Profiles

Delete cached copies of roaming profiles √

After the student logs off the system, we need to delete all traces of the secure login so students cannot figure out the details of how the security is implemented.

Automatically detect slow network connections √
Slow network connection timeout: 10000 √
Slow network default profile operation: Download profile √
Choose profile default operation: Download profile √

These last four items are related to ensuring that the profile is downloaded in all situations.

Extreme care must be taken when changing default policies in Windows. Do not change any other policies available in the policy editor unless you are very sure what you are doing. You may open the computer to further attacks from the Internet. It is even possible to create a set of policies that lock out the administrator from changing policies (this happened to the author while learning about policies)! In that case, the only fix is to reinstall windows.

Controlling Access to Web Sites with Content Advisor

Another security hole in browser-based on-line testing is control of web access by the students. Otherwise, a student could visit a site and possibly find information to help with the test questions or even build their own site to use as a “cheat sheet”. A student could also use a web-based e-mail system to communicate with other students in the class or someone outside of the room. On the other hand, the computer must still allow access to at least the site hosting the on-line assessment. In addition, the instructor may wish to allow access to a select list of web servers.

The solution to this problem is to use Internet Explorer's "content advisor" to control access to web servers[6]. This is a two-step process. First, Internet Explorer must be configured to block access to **all** web sites. Then the site hosting the assessment is added to the "Approved Sites" list in Internet Explorer. Any other sites that the instructor wishes to allow access to can also be added at this point.

First a special text file (a ratings file) is created which tells Internet Explorer to deny access to all web sites[2]. This file is then placed in a folder contained in the server's copy of the user profile (discussed in the next section). That way the ratings file is automatically downloaded during login and is in a specific location. Next, Internet Explorer is configured[2] to use this ratings file. Then it is configured to allow any web sites that the instructor wishes students to have access to.

To further increase security, JavaScript can be used to open the assessment in a new window in "full screen" mode with no toolbars visible[7]. This prevents students from accessing other sites via toolbars. The assessment must have a means of closing the assessment window though since there is no close box on a window opened in full screen mode.

Controlling Access to Computer Resources with Profiles

Microsoft's solution to managing multi-user systems is the user profile. A profile stores two different types of information about the user:

1. User specific registry settings and
2. User specific files and folders

The registry settings contain information on any preferences that the user might have set in programs. In our case, this allows us to configure Internet Explorer to use content advisor to block most of the web and have these settings automatically applied during login.

The user folders contain user specific storage. These include the desktop, cookies, "My Documents", "Start Menu", Favorites, and any other user specific storage that programs might require. If the on-line testing system allows checking of cookies as part of the connection process, then any necessary cookies can be placed in the "cookies" folder and they are automatically available to the assessment system. In addition, the ratings file for Internet Explorer's content advisor can be placed in any of these folders. It is then downloaded and available for use after login.

There are two different types of user profiles, roaming and local. A local profile is stored on the users local computer and would require the pre-installation of a local profile to use the secure on-line assessment system. Instead, a roaming profile is used. This profile is stored on a Windows domain server and downloaded during the login process. In addition, a roaming profile can be made "mandatory" which means the user cannot change any settings. Thus, by using a mandatory roaming profile, the student's computer can be automatically configured at login to be secure without having to pre-install any applications on their computer.

Internet Explorer on a client computer must also have some configuration done. Since Internet Explorer is the default program (due to a policy setting) and the list of web sites that can be visited is restricted, the homepage should be configured to be the web site that hosts the assessment. To improve security, it is also a good idea to delete all cookies and the cache files on the client computer.

Creating a user profile for secure on-line testing is a three-step process:[8,9]

1. Configure the local computer as desired
2. Create a copy of the profile
3. Move the profile to the correct location on the domain server

Copying the appropriate profiles folder in Windows explorer will result in a profile that does not work properly. The problem is that the permissions on both the folders in the profile and more importantly, the user's registry settings will be incorrect. Instead you must use the User Profiles tool in the system properties control panel[4].

Once the configured profile is finished, changing it into a mandatory profile is straightforward. All settings for a roaming profile are stored in a file named "Ntuser.dat" (on windows NT). Renaming this file to "Ntuser.man" changes the profile into a mandatory profile. A good detailed step-by-step tutorial is available for creating this profile.[10]

The User Experience

Before the system can be accessed, the student's computer must first be added to the domain server. The domain administrator must be present the first time a student logs in to add the computer to the domain server. This is best handled at the beginning of the term in the classroom. Only one special account needs to be created by the domain administrator for taking assessments since all students share this same login.

After the student logs onto the Windows domain server, the downloaded policy and profile configure the student's computer to replace the desktop with Internet Explorer. This is configured to use the assessment web site as the home page. Access to other web sites is blocked unless the instructor has configured the profile to allow specific exceptions. There is no desktop on the computer, only a blank blue screen. Even if the student quits Internet Explorer, there is only a blank blue computer screen. Access to other programs on the computer is blocked unless the instructor explicitly allows exceptions.

The rest of the configuration is related to preventing students from modifying their computer to work around the security system. The task bar is gone, there is no start menu, contextual menus for the desktop are missing, plus many behind the scenes settings prohibit students from hacking into prohibited resources.

After the assessment is complete, the student only needs to log out of the domain and back into their computer as a local user to completely unlock the computer.

Testing Results

This secure testing environment was tested in a sophomore class of 25 engineering students. All students had had at least one course in programming and the use of Microsoft Office. Their level of computer expertise varied from using applications only to one student who worked in a windows support capacity as part of his job.

The entire class was asked to simultaneously log into the Windows domain server using the secure account. All logins completed quickly with no appreciable delay before the browser was available. The students were then asked to try and access other web sites and software on their system. None of the students were able to by-pass the security safeguards in place. Then they were asked to try and access any other resources that they knew were on their computer. In all cases, no one succeeded in doing any activities other than browsing the selected web server.

Finally, the department's computer support person was asked to login to the secured account and attempt to access web or local resources other than those on the allowed web server. This person is responsible for maintaining over 200 windows computers. In addition, he also maintains the windows domain server used in the testing of the secure login. Even with over fifteen years of experience in supporting windows systems, he could not access any resources other than those allowed by the secure login.

Conclusion

The purpose of this project was to develop a secure on-line assessment method that was:

- As secure as traditional paper and pencil testing
- No additional applications installed on the student's computer
- Inexpensive
- Easy to implement

The final solution consisted of using a Windows domain server to process student logins during which a custom policy and profile were applied to the student's computer. After logging in, the student only saw Internet Explorer on their screen. This system only allows access to those computer and Internet resources that the instructor wishes to allow the students to use during the assessment. Although a free custom ratings file is automatically downloaded, no applications need to be manually installed on the student's computer. There is no additional cost involved if a Windows domain server is available to the instructor. Finally, this system is easy to implement.

During an assessment student's cannot use any email clients, visit any web-mail based systems, run any instant messenger programs, run any prohibited software, can only visit approved web sites, and are stopped from hacking the security system to circumvent these prohibitions. No students have yet succeeded in bypassing a secured computer.

Bibliography

[1] Ensuring Students Have the Prerequisite Skills for a First Course in Engineering, Fred E. Weber, John W. Prados, ASEE Summer Meeting, June 2003.

[2] Cheating in Online Student Assessment: Beyond Plagiarismhttp. Summer, 2004. 3 Jan. 2005. <http://www.westga.edu/~distance/ojdla/summer72/rowe72.html>

[3] Perception Online Assessment, Unknown, 20 Feb. 2005. < http://www.pearsonncs.com/perception/index.htm>

[4] Assess, Observe, Understand, Act, Unknown, 20 Feb. 2005. http://www.eyecues.com/assessa/

[5] User Profiles On Windows 2000 Workstation. 1 Jan. 2000. 2 Jan. 2005. <http://www.lsa.umich.edu/lsait/TrainingDoc/Documents/Win2k/User_Profiles.doc>

[6] How to Configure Internet Explorer 5.x to Block Access to All But Approved Internet Sites. 9 Sept. 2004. 2 Jan. 2005. <http://support.microsoft.com/?kbid=267930>

[7] HTML and DHTML Reference. Unknown. 4 Jan 2005. <http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/open_0.asp>

[8] User Profiles On Windows 2000 Workstation. 1 Jan. 2000. 2 Jan. 2005. <http://www.lsa.umich.edu/lsait/TrainingDoc/Documents/Win2k/User_Profiles.doc>

[9] Guide To Windows NT 4.0 Profiles and Policies. 17 Nov. 2003. 2 Jan. 2005. <http://support.microsoft.com/kb/161334/EN-US/>

[10] How To Create a Roaming User Profile in Windows 2000. 15 Jul. 2004. 2 Jan. 2005. <http://support.microsoft.com/default.aspx? scid=kb;en-us; 302082>

Biographical Information

DR. FRED WEBER

Fred Weber is an Associate Professor and Associate Head of the Chemical Engineering Department at The University of Tennessee. He received a BS in Chemical Engineering from the University of Michigan in 1974 and a Ph.D. in Chemical Engineering from the University of Minnesota in 1982.