HOW TO RECEIVE AND PROCESS ATTACHMENTS WHILE GREATLY REDUCING THE RISK OF VIRUSES AND TROJANS.

Roy F. Cabaniss
University of Arkansas Monticello
cabaniss@uamont.edu

Ron Portis
University of Arkansas Monticello
portis@uamont.edu

ABSTRACT

When you are teaching an online or distance learning course you often need some safe means of transferring files. Few things are more discouraging than to have received a file which managed to shut your system down. What follows is a walk through for students for transferring files and a guide to the instructor for file and computer safety and security concluding in a process for establishing a safe mechanism for receiving and grading papers which will keep your office computer safe.

INTRODUCTION

There I was teaching a distance learning class and the students were e-mailing their homework to me. As I opened the files to grade their work I did not give much, if any thought to systems security. However, the next day, when my computer refused to boot, not only was system security on my mind, but it was accompanied by that sinking feeling in the pit of my stomach and the thoughts of "oh lord.. a virus" and "how much work am I about to lose."

The recent experiences with SoBig and Blaster have turned knowledgeable systems administrators and computer users to consideration of what are called "Day Zero" viruses or worms. It is a fact that anti-virus software is only as good as the data file which contains the patterns of the known viruses. A "Day Zero" virus is simply one for which the pattern is not known. Such a virus would not be stopped at all by any anti-virus software. Thus the importance of receiving regular updates of your anti-virus data files. The more viruses the anti-virus companies find, the more patterns they can put into the software to be recognized and the more viruses are stopped from harming your computer.

This is a very compelling reason to use Linux for some of your teaching tasks. **Viruses are operating system dependent.** Look at the recent problems with Blaster. It attacked windows XP and 2k and 2k3 and left Windows 95, 98 and ME totally alone, to say nothing of computers running Linux, Unix and Mac OSX. For a virus to be effective, it must be on the operating system for which it was designed, otherwise, its presence is of little consequence and the virus can be removed without harming your system. Since the vast majority of viruses and Trojan horses are written for windows operating system, not running that operating system avoids the problems associated with those viruses.

SETTING UP THE SERVER AND FILE ADMINISTRATION.

There are several ways you can set up a Linux server as a secure repository and Cabaniss (2002) addressed the basics of creating a web accessible server. The simplest setup (and the one we recommend) is to simply create an account on the server for every student you teach. The students deposit their files on the Linux box and you read those files while logged onto the same server. In this way, the files in question are never actually on (or are executed by) your computer and thus are no danger to your system. In other words, regardless of the operating system which is running the computer on your desktop, you will actually be working in Linux on some other computer. The files in question will never have the ability to contaminate your computer since your computer is never actually involved in the processing of the files. The current course management offerings (Blackboard and WebCT for example) do not have this ability since your ability to work with the files requires they be on your computer.

When you set up a student account two directories are usually created. One directory is Documents and the other public_html. In the Documents directory the students will deposit everything which they are turning in which is not a web page or designed for web access. The public_html directory exists for everything which should be viewable from the web. These directories are created by default and do not require your intervention.

Once the student has an account set up you need to ensure the students all have the same software. This allows you to hand the students an instruction sheet (Appendix 1) to guide them through the process of installing the software and your preferred document control. There are many programs which a person needs to deal effectively with the web. Some of the necessary programs are not installed when an operating system is installed but all of them can be found for free if you know where to look . The easiest way to distribute the software is to have the students give you a blank CD and you give them one which has all the programs on it. All of the programs which this article addresses (and many more) are contained in the iso image under the teaching materials link on the authors website (http://cabanisspc.uamont.edu/) and may be freely downloaded and burned onto cd's.

The first thing you will want/need to do is to get a copy of the software for the platforms your students are running. It does no good to require software which must be run on XP if the student only has Windows 98 so the software must be capable of running on a minimal machine and OS. The set of software we recommend is in Table 1.

Table 1: **Software**

Software	***Client OS***	***Windows***	***Linux***	***Mac OS X***
Telnet		Putty	Xterm	xterm
SSH		Putty	Xterm	xterm
FTP		WS FTP	IglooFTP	IglooFTP
Editing / Office Suite		Openoffice for Windows	Openoffice for Linux	Openoffice for MAC OS X
Archive		Winzip	Zip	zip
Remote desktop		TightVNC	Vncviewer	Vncviewer
IRC / Chat		Mirc	Kvirc	kvirc

THE PROCEDURE FROM THE STUDENT'S PERSPECTIVE.

From the student's perspective matters are rather simple. The student will do their work and then ftp the files to the appropriate directories on the Linux server.

When comparing an online / distance learning environment to a traditional classroom, one additional thing which must be considered is the file format. Whenever you save your work from a program, the computer encodes the work in a specific fashion, this encoding being called the file format. This is why you can receive a document that looks like it is all in machine code and the sender insists that the document is normal, the document was saved in a format that your computer cannot translate. File formats get even trickier when you consider the fact that even within a program files can be mutually incompatible between versions (MS Office 97 cannot read MS Office 2k for example). For word processed documents a very reliable standard is called rich text format. Rich text format documents can be read by any modern word processor. Some suggested file formats are given in Table 2.

Table 2: Suggested File Formats

Software	***File Format***
Microsoft Office Suite	MS Office defaults (doc, xls, ppt)
Lotus Wordpro, Wordperfect, MS Word	Rich Text Format (rtf)
Lotus 123, Quatro Pro, Excel	Excel (xls)
Powerpoint	Default (ppt)
Openoffice	Default

The Openoffice suite has the ability to read all of the Microsoft office default file formats and also save documents in those formats so if your students are in a Microsoft only environment, simply staying with their defaults is an option. Alternatively, if the students working with Openoffice and saving the documents in Openoffice format, the version control options of Openoffice make grading and marking up papers easier with the ability to insert color coded comments where desired.

When the student has completed the work, then all they need to is FTP the completed assignment to the appropriate directory. Instructions for FTPing are given in the Appendix.

THE PROCEDURE FROM THE FACULTY MEMBER'S PERSPECTIVE.

If you are at the desk with the Linux server nearby grading the papers is easy. You simply go to the server, login and evaluate. Nothing goes onto your desktop so it stays safe.

The more common situation though is if your desktop is separate from the server. In that case you want to remotely log in and graphically interact with the server and documents stored therein. There are multiple ways to accomplish this but one of the easiest is to establish a virtual network connection (VNC).There are other ways which establish a much faster connection, however in many instances they are operating system dependent. As far as the author has been able to establish, you can set up a vnc with all operating systems. A VNC has the advantage of working on virtually all operating systems and securely through most firewalls. When you are using a VNC it is as if you are sitting in front of the computer with the exception being that an Ethernet connection is not as fast as a keyboard plugged straight into the box. In technical terms, a VNC makes the computer in front of you work as a thin client.

To read and grade the web accessible documents you start a browser and surf to the Linux server's address and into the students accounts. (http://your.server.name/~student_accountname). What they have deposited there is visible for grading.

The non-web accessible documents are readable by Openoffice. You login via a VNC and then start Openoffice on the server. With Openoffice running you go to the directory where the student deposited the files and read the documents. (It is very possible to set things up in such a fashion so that you can comment and markup their papers also.)

CONCLUSION:

The result of the preceding process is that potentially contaminated files are never on your computer and do not risk infecting your machine. Therefore you do not run the risk of losing time due to hostile programs. An additional component would be to make the Linux server scan all files on it on a regular basis for hostile intent.

BIBLIOGRAPHY

Cabaniss, Roy F., (2002) "How 2 setup your office computer to run Linux for teaching e-commerce without messing everything else up." Developments in Business Simulations and Experiential Exercises, eds. Mary Jo Vaughn, Pensacola, Fla.

APPENDIX 1 STUDENT INSTRUCTIONS

First of all your web accounts have already been created. The following is a walk-through of the process of getting the account finalized. For these instructions,
“~” means to click a selection,
“T” means type what is in the " quotes " (Don't type the quote marks)

You account was created with the first initial of your first name and the first five letters of your last name and two numbers. So for me for example, my account is rcaban01.

INSTALLING THE PROPER PROGRAMS TO YOUR COMPUTER.

Put the handout cd in your computer.

~	My Computer
~	Whatever letter your cd drive is
~	the winzip folder
~	winzip.exe and let it install
~	Back
~	ftp
~	ws_ftple.exe and let it install
~	Back
~	Java
~	j2re-1_4_0_01-windows-i586.exe and let it install
~	Back
~	Back
~	C drive
~	Program Files
~	File
~	New
~	Folder
T	“Putty”
~	Back
~	Back
~	CD Rom Drive
~	putty then copy putty from the cdrom drive to its directory on your hard drive.

OPTIONAL BUT HIGHLY RECOMMENDED. If you want Openoffice installed

Go into the Openoffice directory on the CD.

~	Ooo_1.1.0_Win32Intel_install.zip and let winzip install Openoffice. Depending on your computer configuration, you might need to point the install to the Java directory in c:\\Program Files\Java\j2re1_4xxx\ .

RUNNING THE PROGRAMS

The main (and in many instances only) new program the students must be involved in is their ftp client. If the students are working with Microsoft office and that is the file format desired for turning, then they should continue doing so.

TO TRANSFER THE FILES TO THE SERVER SO THEY CAN BE GRADED.

~	Start
~	Programs
~	Ws_ftp
~	WS_ftp95 LE
T	the name of the Linux server On the hostname line (must be in a DNS)
T	the students account name On the username line
T	the students account name On the account line
~	Ok

The left side of the display is your windows box, the right side is the server where you will deposit your work.

Move your mouse to the right side and

~	Refresh

PICK ONE

~ Documents if what you have is not a web page or for Internet viewing. (written assignment, term paper, spreadsheet etc.

or

~ public_html if what you have is seen from the Internet. (web page, php, database, asp etc.)

Move your mouse to the left side and move among the directories until you find the file which you want to turn in.

~ the file to be turned in

~ the arrow pointing to the right in the very middle of the program.

Congratulations, the file is now posted and ready for grading

TO CHANGE YOUR PASSWORD

~ putty

~ ssh

~ connect

~ remote system

T "cabanisspc.uamont.edu" on the host line

T whatever your account name is

T "passwd"

T "student" (when it says old password) That is to give you a new password for this account. It will ask you for your new password. If you are successful it will say password changed. If is does **NOT** say password changed keep trying. We have set this up for secure passwords, so words and names will usually not suffice as passwords.

Close Putty

FACULTY INSTRUCTIONS

There are equivalent commands in all of the major Linux builds. In particular SuSE, Redhat and Mandrake all have an equivalent. The instructions which follow are first given as generic and then SuSE (I list the SuSE instructions because that is the build of Linux I am using as I write this.)

~ means to click a selection

T means type what is in the " quotes " (Don't type the quote marks)

GENERIC ADDING A USER (STUDENT)

~ Whatever icon you have to bring up your menu. In the menus available one of the choices will be something for systems administration. This will require the root password. What you want to do is to add a user to the system.

CONSIDERATIONS

1. Every student will get their own account as a normal user.
2. Use some form of standard naming system.
3. Allow them no more than one login before they must change passwords.
4. Enforce password checking.

ADDING A USER USING SUSE.

~ the far left icon on the bottom panel.. the one that looks like a smiling chameleon

~ Systems

~ Configuration

~ YAST

T the root password, whatever you set it to be

~ Security and Users

~ Edit and Create Users

T The students first and last name in the blocks provided.

T The username. This is the name the computer will allow the student to login as and you should use some form of standard naming system. It is important to remember that YOU set the username, not the student. Don't worry about making it convenient for them, make it workable for you. Standard naming systems include the first initial of the first name, first five letters of the last name and a two digit number. For myself for example this would translate as a username of rcaban01. This gives us

room for 100 J Smiths and is easily expandable to 999 of them.
T A standard password for all students. I use “student”.
~ Finish

ESTABLISHING A VIRTUAL NETWORK CONNECTION (EVERYTHING IS CASE SENSITIVE)

~ putty
T your hostname for the Linux computer on the hostname lines
~ ssh
~ Open
T your username on the Linux computer
T your password on the Linux computer
T “vncserver”
note what it says the X desktop name and number are. Note, as long as the Linux server is not rebooted, you do not need to start a new vncserver.
T “exit” (closing out putty)

EVERY TIME

~ Start
~ Programs
~ Tightvnc
~ TightVNC viewer
T the X desktop name and number on the vnc server line
T the vnc password (you set it the first time you typed vncserver)
~ the Openoffice icon
start working.

Appendix 2 (optional for inclusion.. sometimes it helps to explain terminology)

JARGON TRANSLATOR (very tongue in cheek)

Database: A way of organizing data and getting to the information.

Defrag: A windows program to logically organize your hard drive. Linux does this automatically.

Directories: Basically a computers file cabinets. If you want a neat office, you put your papers in the file cabinet instead of scattered all around on the floor. Same Principle.

DNS: The phone book for the world. It associates a name (cabanisspc.uamont.edu) with an ip number (204.126.114.182). Remember that computers only use numbers.

E-commerce: actually achieving buzzword status, but basically this encompasses any forms of doing business wherein the interactions are between two machines. (IE, you buying things on the Internet on e-bay, or a store automatically reordering items through their edi interface.

File Format: The way one program knows how to interpret what it already wrote.

Firewall: Either hardware or software which exists to keep non-authorized persons from doing anything to your machine. (Ps, the software solutions Imo are better.)

HTML: Hyper Text Markup Language: Actually plain text writing with commands (also in plain text) built into the pages. Almost all modern word processors have the ability to save a document as an html file. Normally, these are incapable of dealing with the technical commands associated with database interactive web sites.

IP address: how the outside world can look up your particular machine out of all the computers in the world.

Kernel: A techie term for the real operating system behind the marketing hype. The machine code that actually makes the operating system what it is.

Kernel 2.4.10: In the Linux/Unix world revisions and modifications are constantly being made. So you have to have a way to keep things constant so that person A knows if person B is working with exactly the same thing. This is done via a numbering system. The first number is the main build number. These change very very rarely. The second number tells if it is a stable (it won't crash that often) or experimental release. If the second number is even, it is stable. If the second number is odd then the kernel is developmental and there is no telling what they are doing with it. The third number is telling you the specific version you are working with. The specific versions associated with a reseller of Linux (SuSE 7.3 versus Redhat 8.0) mean almost nothing, it is the kernel numbers that matter. So if I am using SuSe 7.3 which has kernel 2.4.10 and you are using Mandrake 8.0 with kernel 2.4.8 what matters is the kernel numbers, not the SuSe or Redhat or Mandrake numbers.

LILO: A program that will let you choose the operating system that you want to start up with when you first turn on the machine.

Linux: A free Unix clone (operating system).

Operating System: What makes a computer a computer. The software that you actually interface with. Windows 95, Windows 2000, Linux, Unix, BSD, MSDOS, DRDOS, Solaris, HP-UX are a few examples.

Perl: A computer language that is used a LOT by Linux folks. Very compact with tight code and comparatively fast execution.

PHP: A scripting language for creating web pages and accessing databases. Not pretty but lordy is it fast.

Punch a hole: To open a specific port number in the firewall for a specific type of Internet query to go through.

Scandisk: A windows program to see if your hard drive is OK. Unnecessary in Linux.

Scripting Language: A particular way of getting to the database or executing a program, usually done by writing lines of specific commands in a specific form the computer is looking for. With php for example I first have to tell the computer "look for php code" and then give it the code it is looking for in a very specific format.

SQL: Structured Query Language. A way of communicating with your database beyond cursing. Actually a relatively standardized set of commands that are pretty much identical between ALL SQL databases, including the windows ones. Always use an sql database. It means that the code which you write will be useful later when you change.

Thin Client: A computer that is acting solely as a terminal for another computer.

TCP/IP protocol: The way that Internet computers communicate. The protocol is set on an international basis, so if your computer is working with tcp/ip you will be fine.

Web Server: The part of the computer that makes web pages available to the outside world.