Global Information Assurance Certification Paper

Unique security challenges in Higher Education -

Securely integrating student-owned computers into your network

September 26, 2001
Kerry Vosswinkel
GIAC GSEC Certification – Version 1.2f

The balancing act between freedom and security is a delicate and difficult one. It's certainly not a new one, and is tested in the physical and political arenas as well as in the Information Security field every day.

Higher Ed is not walking this wire alone, of course. Businesses also must balance the needs of the users to accomplish their work with the security and stability of the network. But Higher Education does face some unique challenges – if not in concept, at least in their scope.

Most business organizations have complete control, or at least a large measure of control, over the computers that are connected to their network. They are usually purchased, configured, and maintained by the company, and strict rules and policies govern their use. This is not the case in the world of Higher Education today.

The explosion of broadband access in the residence halls has resulted in a large part of the network being comprised of computers neither owned nor managed by the college. These computers, moreover, are being used in learning environments, where a student who wants to learn how to install an NT server or set up a network may choose to do so on his own machine.

Securely integrating student-owned computers

From ABCNews stories[1] to articles in on-line publications such as *Yahoo! Internet Life*[2] and convergemag.com[3], it is widely recognized that one of the largest populations in the US with access to high-speed Internet connections are students living in college dorms. Many campuses even require incoming students to own a computer. This means that at the start of each Fall term, thousands of students bring a computer up to campus and plug it in to the network.

Anyone who has children or has ever worked in a school knows that the beginning of each school year is a signal for a new crop of cold viruses to begin their spread. On the wired campus, not only can **you** catch a virus, your network can also. With the growth of broadband access in the home, the extra exposure of always-on connections when students have their computers at home between terms, on connections that may or may not be as secure as your own network, insures that the problem will only get worse.

In the early days of computer viruses when the transfer mechanism was typically a floppy disk, the damage was localized. Perhaps files on the hard drive would be deleted, or programs would misbehave, but unless it deleted your homework and you had no backup (sadly, an all too common situation) the effects weren't catastrophic and certainly they weren't widespread.

Modern "malware", the current catch-all word for viruses, Trojans, worms, and other software specifically designed to damage or disrupt a system, is much smarter, spreading incredibly quickly via e-mail address books, and actively searching for unprotected network file shares or unpatched systems with known security holes.

Defense in depth, the practice of layering defenses to provide better protection, is a critical approach in information security today. Organizations that have strong perimeter defenses, constructed from products such as firewalls and antivirus software on mail and internet gateways can secure their networks fairly well from outside attacks. But what do you do when the malware bypasses your walls and walks right in the front door, already running on your student's computers?

There are five things you can (and must) do:

- Specifically address student-owned computers in your policy
- Train your students in security awareness
- Restrict access to your systems
- Monitor your resources
- Have an incident response plan

Policy

"Keep it Simple" is the golden rule that should apply to security policies in general. Since the size and complexity of a policy is inversely proportional to the likelihood of its being read, I recommend that a specific, concise section of your policy be devoted to student computing. Here are the basics:

- Do's
- Don'ts
- The consequences of Doing a Don't

That seems almost too simplistic, but it really does cover all the basics. At the college where I work, for example, our policy "Use of Student Residence Computing Networks" can be boiled down to the following:

- Do's
    - Comply with the Student Instructional Computing Responsible Use Code, Conduct Code, and other related college policies
    - Accept responsibility for your content, including complying with Federal and State laws.
    - Follow specified computer naming conventions to avoid network conflicts
    - Be responsible for security, and for activities conducted to or from your network connection.
- Don'ts
    - Assign your computer a non-college-owned domain name
    - Use your computer for commercial purposes (if you are a public college, state laws generally prohibit the use of state-owned resources for commercial purposes)

    - Overload the network
    - Conduct illegal activities
- The consequences – in order of increasing severity
    - Disconnection of the offending computer from the network
    - Disconnection of the entire subnet from the network
    - College disciplinary action
    - Criminal prosecution

Security Awareness Training

Teaching your users the basics of information security is one of the most important things you can do. Moreover, a college is a natural place for such teaching, since that is our primary function. It should be an ongoing process, in cooperation with the campus housing staff if possible, for a couple of reasons:

- They know the students better than you do. This is extremely important, since teaching is an art perhaps even more than a science, and the cooperation of people who know your target audience may make all the difference in your success.
- They are less likely to use "geekspeak" that might confuse or bore the audience. Ask them to call you on it if you do.

Try to space out your teaching efforts – incoming freshmen and transfer students are already overwhelmed with information at the beginning of the term, so offer activities throughout the year, perhaps via contests or other reward-based activities that encourage students to participate.

Teaching a student how to protect their own computer provides multiple benefits

- Students will be better "netizens", preventing their computers from being used as launching points for attacks on your own system or others.
- Students are less likely to have their computers compromised during term breaks when the computers are removed from your network and connected to another, perhaps less secure one.

So what are the basics that your students need to know? The CERT Coordination Center recently published a document that instructs users of broadband connections in the basics of computer security[4]. That document, while all-inclusive and detailed, may well be above the heads of most casual computer owners. It did provide some of the basics for the list below which, while not as comprehensive, is at least a good start. You may add others as you see the need.

- E-mail security.
    - If your e-mail client software allows automatic opening of e-mail attachments, be sure to turn it off.
    - Never open attachments that you are not expecting, even if they appear to be

from someone you know.
    - On Windows systems, do not hide file types for known file types. This very dangerous default setting can hide the fact that a file is executable – for example, a file called openme.txt.com will appear as openme.txt, allowing harmful executable attachments to masquerade as harmless types like .jpg or .txt
    - View mail as text only if possible. If you do view mail in HTML format, configure your e-mail client so that it doesn't allow scripts to execute.

- Internet security
    - Install an anti-virus program on your computer, and keep it updated. Most modern antivirus programs have one-click, or even automatic, update features – use them!
      As an aside, if you choose to provide your students with antivirus software, be careful when considering use of a centrally-managed version, where updated definition files are distributed from your servers. Though it's tempting to be assured that it is installed on all computers and updated regularly, automatic distribution of software to computers the college does not own is risky. It may cause conflicts with already-installed software, and will certainly cause problems when the computer is removed from the campus network when the student leaves.
    - Disable file and printer sharing.
    - Exercise care when downloading anything from the Internet. It is an excellent source for free or low-cost programs, tools, games, etc., but it is also an excellent distribution source for the latest malware. If your antivirus software does not have a dynamic component, that is "always on" and running background scans, be sure to run one manually before executing any program you've downloaded.
    - Keep up-to-date on software security patches. Windows Update, for example, is built in to the latest versions of Microsoft Windows operating systems and Internet Explorer – though it doesn't completely automate the process (and it's wise to be leery of programs that execute any actions on your behalf without asking first), it does provide quick links to the latest patches.
    - Install a personal firewall. Recent articles on SecurityPortal.com[5] and in Information Security magazine[6] review many of these products. Two of the most widely recognized are Zone Labs' ZoneAlarm and Network Ice Corp.'s BlackICE Defender. Personal firewalls are excellent tools for both users and administrators, and will be referred to again in the section on monitoring your system.

- Social Engineering
    - Security breaches are not always technical – the weakest link is often human. Gullibility, curiosity[7], and some very common human desires: to be helpful, to trust others, to appear competent, to be attractive to those we admire or desire, and many others[8], can all be exploited by crackers intent on compromising your systems. Make your students aware of some common social engineering techniques – make sure they also know those techniques are never used by your own computing staff (for example, that a student will never be asked for their

password via telephone).
    - Social engineering can have technical components as well[9]. For example, Javascript can be embedded into a page and cause a popup window to appear, implying that the user has lost his network connection and requesting the username and password for reconnection. This information could then be e-mailed to the web-page author.

- Account and Password security[10]
    - Accounts should never be shared. Give good reasons for this – how would a student feel, or even more importantly defend himself or herself if their account was used to commit a crime, and their account "fingerprint" was found in all the log files.
    - Passwords should be "strong". There are many sources for creating strong passwords, but most agree on the following:
      * Passwords should be reasonably long – most recommendations say that 8 characters should be the minimum
      * Passwords should be composed of a mix of characters - letters (both upper and lower case), numbers, and special characters.
      * Passwords should never contain any part of the account name, nor should they be words that appear in any dictionary (in any language), names of friends, family or pets, birth dates, Social Security numbers, or any other commonly known or easily discovered personal information
      * Don't rely entirely on common number/letter substitutions like 0 for o, 1 for i or l, and 3 for e – these are widely known and may not provide much additional security

      A common suggestion for creating a strong password is to start with a phrase that has meaning for the user, and construct the password from the initial letters of words with appropriate numbers and special characters interspersed.
    - Passwords should never be written down. A strong password is worse than a weak one if the user must write it down to remember it.
    - Passwords should be changed at regular intervals. 30 to 90 days seem to be standards that are often suggested. Passwords should be changed **immediately** if there is reason to believe they have been compromised.

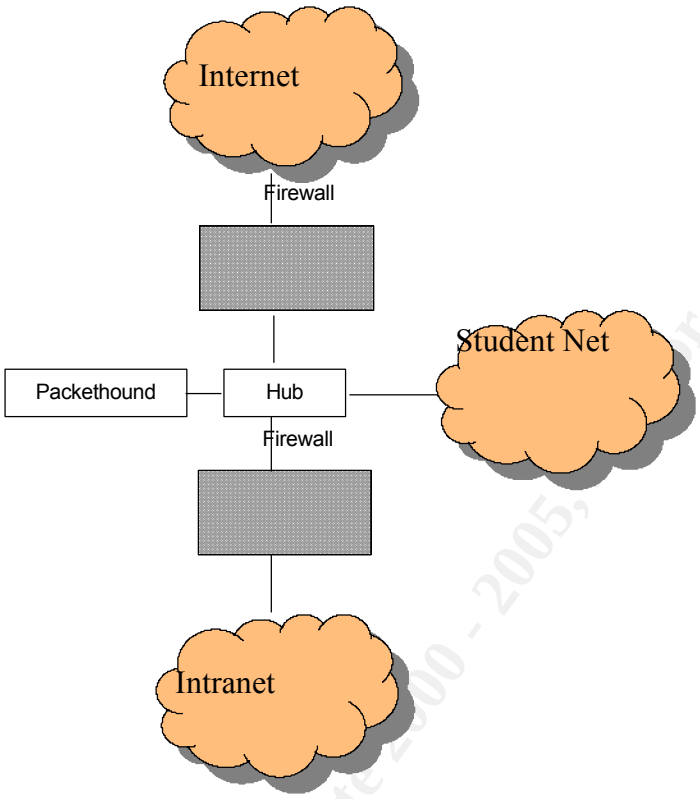
Restrict Access

Restricting access between the uncontrolled, or lightly controlled, segment of your network comprised of your student's computers, and the more secure academic and administrative segment can be accomplished in a couple of different ways. Utilizing the defense-in-depth strategy again, the two most likely areas to address are network design issues (both hardware and software), and hardening systems.

Network Design

A thorough examination of components and design for a secure network are beyond the scope of this paper. However, some of the basics that should be considered are:

- Single- or multi-domain networks
  Single domain networks are much easier to administer, generally less expensive to



  implement, and more user-friendly as well. They are unquestionably less secure, however, since a compromised account has access to resources across the entire network instead of on a single machine or a local domain.
- Network topology
  Switches, routers, and firewalls are the most common hardware components of networks today. VLANs can be used segregate traffic between logical networks, perhaps routing that traffic through a firewall first. Even without a firewall, routers can be used to implement some security via mechanisms like Access Control Lists (ACLs). Cisco, for example, has a very detailed publication on router security features – both on securing the router itself, and on using the router in helping secure your network[11]. Implementing some of the security features on routers may result in slower performance, however.

- The DMZ is growing in popularity as a way of separating networks into different security groups[12]. The most common use is to provide an extra layer of protection between "public access" computers like web and DNS servers and your intranet, but you could use a similar strategy to semi-isolate your student network. Figure 1 above shows a sample layout, which also uses PacketHound™[13] to increase security by monitoring, logging, and/or blocking packet traffic between the three networks.

  The most secure configuration would undoubtedly be a completely separate network for student computers, with completely separate routers and firewalls. If the only network services provided to students are e-mail and web-browsing, this may not be a bad choice, provided you kept the student e-mail server in their own network. However, if students need to access software hosted on your academic or administrative network, such as software provided in student computing labs, a separate student network would not really be practical. It would, for example, make it impossible to implement security features like ingress filtering, since you would have to allow college-owned IP addresses to come in "from the outside" through the firewall outside your intranet.

Network design is an important part of the defense-in-depth strategy, but it is only one part. In Higher Education, particularly public colleges and universities where budgets are nearly always tight, you don't necessarily have to spend a lot of money on network devices such as multiple firewalls. If you are vigilant in hardening your systems, student computers and accounts should have little access to critical systems.

Hardening Systems

To "harden" a system essentially means just what it sounds like – to make it as impervious to penetration as possible. The less control you have over all the computers in your network, the more attention you need to pay to hardening the critical systems you do control.

Figure 1

There are many steps involved in hardening systems, from physically securing the equipment to keeping hotfixes up-to-date for all installed software. The outline below applies to Windows NT / 2000 systems, but though the details will differ the basic principles apply to all operating systems and servers.

The SANS Institute has an excellent publication called *Windows NT Security: Step by Step*[14] that covers every phase of securing an NT server. It not only lists every step, but also gives details on why it should be done and exactly how to do it.

The basic areas you need to address are:

- Physically secure the servers, including protection from booting by unauthorized people, and securing backup media and Emergency Repair Disks
- Secure the file system, using file-level access controls whenever possible
- Secure Registry-related elements. Not only do you need to keep the registry files secure,

since they contain your account information, but many registry keys have security-related functions as well, such as:
    - Setting the logon message
    - Restricting anonymous logon
    - Controlling access to the command scheduler
    - Password related keys, such as the Netware DLL Trojan[15], and the strong password service that was released with NT 4.0 SP2
- Carefully plan your group and user setup, including managing the default accounts and groups (such as Administrator, Guest, and the Everyone group), setting password policies (account lockout, password length and reuse, etc.), and assigning user rights.
- Disable or uninstall unnecessary services or subsystems, and configure the needed ones for maximum security.
- Keep hotfixes, patches, and service packs up-to-date.
- Turn on auditing, not only on the O/S but on web server software.

Turning on auditing, of course is only useful as long as you pay attention to what is being logged. Which brings me to the next section – monitoring.

Monitor your system

"Know Thy System" is a classic phrase in security circles. If you don't know what *should* be going on in your network, how will you detect what shouldn't?

Most students look on their computers as useful tools and not much more – very few of them are, or have any desire to be, security administrators. A well-executed security awareness and training program will mitigate the risks, but their computers are windows into your system, so it's important to monitor activity on your network in a variety of ways.

Turning on audit logs for the O/S and other server software is a necessary element of any intrusion detection program. But logging alone doesn't provide security – you must monitor the logs on a regular basis. This can be a daunting task, since log files are both huge and complex. In all but the most simple networks, you're better off implementing a commercial product designed for this purpose than trying to manually examine the logs. These products have the additional advantage of being able to generate alerts based on criteria you specify.

It's important to monitor at least two classes of logs:

- O/S event logs
  These can be configured to track many types of events that can alert you to potential intrusions. Among the events you should track are failed and successful logons, changes in policy, and file access failures (not necessarily all files, but at least the critical system files). Repeated failures will alert you to break-in attempts. Repeated fairlures followed by a success can alert you to an intruder inside your system.
- Other software logs. If you run web servers (and who doesn't, nowadays?) your web access logs can alert you to attempts to exploit vulnerabilities in your web server software.

Since many of the newest worms are spread via these exploits, monitoring your logs can be a key element in detecting intrusion attempts. Databases are another common class of software that it is helpful to keep access logs for.

Host-based and Network-based Intrusion Detection Systems (IDS) are important tools as well, and not only for monitoring your network. The IDS is a fairly new technology, often considered "not quite ready for prime time" – frequently reported dissatisfactions include a high number of false positives, traffic bottlenecks, and difficulty distinguishing serious attacks from nuisance alarms. But they are improving, as "IDS software vendors continue to refine their products' scanning engines, beef up their signature databases and expand their data-collection and analysis capabilities."[16]. New approaches are being looked at as well, such as Top Layer's AppSwitch, which might almost be considered an IDS for IDSes[17].

Personal firewalls such as Zone Alarm and BlackICE Defender have intrusion detection components that can log and block attacks, so install them on your servers and workstations as well as encouraging students to install them on their own computers.

Port scanners such as Nmap, which are widely available in the hacker community, can also be used to scan your internal network, or your student network. These tools can help you detect vulnerabilities in your network, or the presence of Trojans on systems. Commercial products that do port scanning are also available.

Port scanners must be used with extreme caution, however, and never without prior permission from the powers-that-be, lest you find yourself being accused of hacking. This is *particularly* important if parts of your network are managed by different groups of people.

Incident Response

No matter how secure your network, it's almost inevitable that at some point you will be hacked. Monitoring and IDSes can provide valuable forensic information when investigating the details of an attack, but you must be prepared to respond to an intrusion as soon as it is discovered.

The basics of incident response involve[18]:

- Analyzing all available information to determine the type of attack, what systems were attacked, and what the intruder did
- Communicating with all interested parties about the status of the intrusion. These people may be involved in decisions on data-gathering (what, how, for how long) and what actions to take.
- Collect and preserve all information and evidence related to the intrusion. Make sure everything you collect is securely stored.
- Contain the intrusion – this may involve disabling services, accounts, or file accesses, shutting the system down or disconnecting it from the network, etc.
- Eliminate all means of intruder access. This can range from changing passwords, replacing altered files, and removing any backdoors installed by the intruders to

completely reinstalling the system and restoring data from clean backups, if you can.

- Return the system to normal operation
- Finally, learn from your experiences. What did you overlook that allowed the intruders to gain access to your system, and how can you prevent it in the future?

Conclusion

It **is** possible to bring student computers into your network and still maintain the confidentiality, integrity and availability that are the hallmarks of a secure network. Proper attention to basic areas of information security such as policy, security awareness training, restricting access, monitoring and intrusion detection, and incident response can keep your networks as secure as possible.

One of the best ways to make sure you stay secure is to make an effort to stay educated yourself. Read, read, read – there are many good books, magazines, discussion lists, and internet resources that can keep you up to date on the latest security products, enhancements, and intruder techniques. The time you invest in learning how to stay secure is well spent.

References:

1. Muller, Judy. "The Need for Speed." ABCNews.com, January 27, 2001. URL: http://abcnews.go.com/onair/closerlook/wnt_000125_cl_e-world_feature.html (22 Sep. 2001)

2. "America's Most Wired Colleges." *Yahoo! Internet Life*. October 2001. URL: http://www.yil.com/features/feature.asp?Frame=false&Volume=07&Issue=10&Keyword=colleges (24 Sep. 2001)

3. Green, Kenneth C.. "Living With (and Without) Broadband." Converge magazine, Digital Tweed | Campus Connections. October 2000. URL: http://www.convergemag.com/Publications/CNVGOct00/digitalTweed.shtm (24 Sep. 2001)

4. "Home Network Security." Carnegie Mellon CERT® Coordination Center. August 6, 2001. URL: http://www.cert.org/tech_tips/home_networks.html (18 Sep 2001)

5. Boran, Sean. "Personal Firewalls / Intrusion Detection Systems." SecurityPortal.com, June 14, 2001. URL: www.securityportal.com/cover/coverstory20000717.html (24 Sep. 2001)

6. Bahadur, Gary. "Personal Firewalls Under Fire." Information Security, July 2001. URL: http://www.infosecuritymag.com/articles/july01/cover.shtml (25 Sep. 2001)

7. Komiega, Kevin. "Hacker Tactics Prey on Gullible, Curious." searchSecurity.com, April 4,

2001. URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci537875,00.html
(22 Sep. 2001)

8. Stevens, George. “Enhancing Defenses Against Social Engineering.” SANS: Information Security Reading Room, March 26, 2001. URL:
http://www.sans.org/infosecFAQ/social/defense_social.htm (21 Sep. 2001)

9. Tims, Rick. “Social Engineering: Policies and Education a Must.” SANS: Information Security Reading Room, February 16, 2001. URL:
http://www.sans.org/infosecFAQ/social/policies.htm (21 Sep. 2001)

10. “Choosing and Changing Your E-mail Password”. University of Berkeley, Letters and Science Computer Resources. January 11, 1999. URL:
http://ls.berkeley.edu/lscr/support/faq/tips/content/tip_011199.html (20 Sep. 2001)

11. “Improving Security on Cisco Routers.” Cisco Systems, Inc. URL:
http://www.cisco.com/warp/public/707/21.html (24 Sep 2001)

12. Paul, Brooke. “Building an In-Depth Defense.” Network Computing, July 9, 2001. URL:
http://www.networkcomputing.com/1214/1214ws1.html (25 Sep. 2001)

13. “PacketHound Ptotocol Management Appliance.” Palisade Systems. URL:
http://www.palisadesys.com/products/packethound/ (25 Sep 2001)

14. “Windows NT Security: Step by Step.” SANS Institute, March 5, 1998 (electronic updates distributed monthly). URL:
http://www.sans.org/newlook/publications/ntstep.htm (25 Sep 2001)

15. “Security Issues That May Occur Due to the Way Windows NT Handles FPNWCLNT.DLL.” Microsoft. August 8, 2001. URL:
http://support.microsoft.com/support/kb/articles/q99/8/85.asp (23 Sep. 2001)

16. Briney, Andy (introduction). “New Directions in Intrusion Detection”, Information Security Magazine, August 2001 (2001): 49-50.

17. Kessler, Gary C. “IDS-IN-Depth”, Information Security Magazine, August 2001 (2001): 58-60.

18. “Responding to Intrusions.” Carnegie Mellon CERT® Coordination Center. URL:
http://www.cert.org/security-improvement/modules/m06.html (25 Sep. 2001)