

~ COLORADO TECHNICAL UNIVERSITY ~

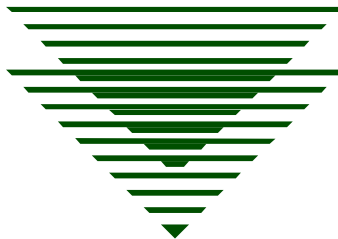
Information Systems Security

Protecting the Network Through Desktop Computer Security

**Professor Karl Seifert
Submitted in Partial Fulfillment of the Requirements for
CS-659
Information Systems Security**

By

**William P. Flinn
Fort Collins, Colorado
October, 2005**



Hypothesis

Desktop computers offer many targets and potential attack entries into an organization's information technology infrastructure. There are many ways that a workstation can be compromised, but by performing some fundamental vulnerability mitigation techniques, workstations can be secured, and the overall IT security program enhanced.

Information Systems Security:
Protecting the Network Through
Desktop Computer Security

When one thinks of protecting a computer network, visions of highly secure firewalls, authentication servers, secure networking systems, and even sophisticated message encryption systems often come to mind. Protecting the perimeter of the network is indeed an important aspect of protecting the network as a whole. Only protecting the outside of the network, however, can leave a large gap in security for an organization's information technology infrastructure. Having a large organization with 7,000 computers, for example, means that there are 7,000 potential targets or ways into the corporate network. By not taking the parts of the systems that are internal to the network (the workstations) into consideration insofar as security is concerned, leads to what is often termed as "bagel security" where there is a hard outside, and a soft, chewy inside. In fact, many users will often perceive their own computers to be safe, as long as the hardened perimeter is there to protect them.

Protecting the network as a whole involves implementing many layers of security. While the perimeter firewalls and routers represent one layer, data encryption may represent yet another layer, it is the security of the desktop computers themselves that represents another equally important layer of security. While firewalls can keep most types of attacks out, they cannot protect internal computers from things brought in through email, or infected files brought in on compact disks or other removable storage devices. Securing workstations involves several processes including risk analysis of what is to be protected, securing the operating system and software on the computer, providing appropriate physical security, and providing education and awareness for end users.

This paper will discuss the idea that workstation security is as important as network perimeter security. This discussion will include the most common types of workstation vulnerabilities, including operating system (OS) vulnerabilities, physical security vulnerabilities, and vulnerabilities caused by the users themselves.

Why Must Workstations Be Secured?

While this paper will discuss some of the processes for making workstations on a network secure, it is first important to discuss why it is even necessary to secure them in the first place. It has been commonly recognized by information technology professionals that computers and other IT assets must be secured for a number of reasons. This has become a very important philosophy due to the fact that so many types and frequencies of computer attacks have come about in recent years. Companies simply cannot afford to take computer security lightly. All of the information technology assets in a network, including desktop and laptop computers, must be secured. Workstations need to be secured because they often contain sensitive information, and are also connected to the network (“Securing Desktop Workstations,” 2003, ¶ 1). This fact alone would indicate that the information on the workstation can be possibly compromised either through theft of the computer itself, or because of an attack that comes in through the network and obtains the information by compromising the machine itself.

Another important reason for layers of security that reach all the way down to the workstation itself is due to the fact that although many attacks can come in from the Internet, a number of attacks can come in from other sources (Panko, 2004, pg. 216). Examples of this include attacks such as WORMS that are already inside the network, and attacks that can be brought in on removable media. Once a malicious file is brought in from the outside and is installed on a computer, an attack can then reach other computers inside the network, especially computers that

have not yet been patched for the vulnerability being targeted. The firewalls and other perimeter security is typically used to prevent malicious software from getting inside, but in this example the malicious software was brought in on a flash drive or compact disk, and the perimeter security had no way to catch and prevent the attack.

Desktop Computer Security – Weighing the Benefits and Risks

There are a number of tradeoffs to consider when contemplating processes for “hardening” the desktop computers. The most fundamental thing that has to be considered is the amount of security needed to protect the workstations. Equally important to the amount of security needed is the amount of performance or productivity that the organization is willing to sacrifice in order to get that protection. The fundamental question of why a workstation must be secured, however, is in that the workstation, being the primary point where actual work is performed, contains all kinds of potentially sensitive material. One other very important issue that has recently surfaced is the widespread use of workstations and other types of computers as what are known as “zombies.” These zombie computers are named such because they represent machines that have been taken over by an attacker and are used in large numbers to carry out attacks on other computers, mainly servers, performing such things as denial of service attacks. These types of computers are infected from a piece of malicious software (Malware) being placed on the computer (Bradley, 2005, ¶ 2). Also, workstations make a target from a physical standpoint in that many users simply walk away from their computers to take a break or to answer an immediate task, or even a fire drill, many times leaving their computers logged in and touching the network. These are just a few of the many examples of why workstations must be secured. As will be discussed later in the paper, attacks can come in to the workstation from the Internet, as well as from within the network. Workstations can be attacked by other infected computers

on the internal network and by unsuspecting users infecting their machines with files brought in on flash drives and CD-ROMs.

Type of Threat – Operating Systems and Software

One of the most vulnerable parts of a workstation is the very operating system that makes it run. The use of Microsoft Windows is extremely widespread and popular as a desktop operating system, and is therefore a likely target of attack (McClure, et al, 2005, pg. 140). This popularity arose out of Windows' ease of use and wide support base. However, it is attractive to many attackers as well because it represents the ability to bring down the product of a mainstream and highly recognized commercial entity. The Windows OS has been exposed to have many holes and vulnerabilities, but Microsoft has done a large amount of work patching those holes and fixing the OS as new attacks are discovered (McClure, et al, 2005, pg. 140).

Other vulnerabilities and threats that can also be grouped with OS vulnerabilities are things such as viruses and malicious software which are used to attack core pieces of the OS or various other pieces of software installed on the workstation. Antivirus and anti Spyware programs are often the target of attackers as well, and much the same as OS patches, must be updated and maintained regularly.

Fixing the vulnerabilities in the operating system can be complicated, but with diligently planned efforts can be very effective. Keeping the OS patched (as well as the other tasks mentioned here) can be a time-consuming endeavor but represents one of the most basic and fundamental (Holden, 2003, pg 29). This involves an ongoing maintenance routine to successfully maintain security. Some fundamental tasks that can be performed include making sure that the OS is regularly patched – that is applying any critical updates, hotfixes, or other patches that are released by the vendor. This should not just include the base OS, but rather

needs to include any installed software as well. A strong antivirus program, including well known antivirus software should be applied, and regularly updated with published virus signatures and other updates. Anti-Spyware utilities have also come into wide production and use as well. These should be installed on workstations and updated along with antivirus signatures and OS fixes.

Type of Threat - Physical Security

Physical security of computer workstations should be a fairly straightforward task, but is often overlooked. One typically thinks of secured access through sophisticated employee ID cards, or even armed guards – which all help the overall physical security picture. However, it is a well known and often discussed notion that many attacks come from within the organization. Curious or even disgruntled employees can pose a risk as long as they can physically get to the workstation. In Ed Tittel's article on physical security policies (2003, ¶ 2) he mentions that any technically or computer savvy person can take over a workstation in less than half an hour in most cases. Laptop computers offer an even greater risk to physical security in that they are small and can be easily stolen. The potential for them to have sensitive data, however, is large. While desktop computers can indeed be stolen from office environments, laptops are even more so vulnerable due to their small size and high value. Since many laptop users are frequently away from their home office, it is likely that a large amount of their day to day working data will be on the laptop. People such as field inspectors and investigators, for instance, are likely to have all of their inspection reports on their laptops. In many instances, this inspection data contains sensitive information. Summarizing, there are at least a couple of very important aspects tied to workstation physical security that have to be considered – preventing the actual physical access

to the computer by unauthorized persons, and the reduction of the potential for theft of the computer, particularly laptops.

In the case of preventing physical access to workstations by unauthorized individuals, one basic measure that can go a long way is for the users to not offer any easy methods for getting into the machine. Having a policy in place such that users are required to either lock their screens or log off the machine when they leave it unattended will have a dramatic affect on reducing the ability of a passerby to sit down and use the workstation. Users should remember that if anyone else accesses the machine that is already logged in, it will appear as if the actual owner of the machine is performing the tasks actually being done by the attacker. Many organizations make it clear that the workstation owner can be held accountable for activities done under their personal login, even if it isn't them.

Type of Threat - End Users

The end users themselves are often a source of security weaknesses. But it should be remembered that in the workplace, it is the end user's job to do whatever business tasks they are primarily concerned with. Security is the task of the IT department. However, it should be noted that a certain amount of user awareness is required in order to keep them safe and minimize their own contributions to computer attack vulnerabilities. Users in the home computing environment are largely unprotected because they are unaware and have little knowledge of the tools that are available to protect their computers (Lemos, 2004, ¶ 1). Still other security issues related to users are such things as a lack of good security habits. Users many times do not lock their computer screens or log out when going away from their workstations. This in itself can lead to a wide variety of attacks from casual (and curious) passersby who can get in and get out before the unsuspecting person returns to their workstation. Then there is always the much joked about

password that is taped to the computer monitor. In some cases, this isn't entirely far from the truth as people have a tendency to write down passwords, particularly if they are required to use complex passwords, and put them where they are easy to lookup.

Users in the business world have the incumbent responsibility to know what their role is with respect to computer security. The IT department is usually the entity tasked with ensuring that user awareness is fostered. But the end-user is still responsible for knowing what tasks they must do (or not do) to stay safe. This would be analogous to a car owner knowing things such as the fact that periodic maintenance has to be performed on their car. They must know how and where to go to check the oil and the tire pressure, but don't necessarily have to know how to disassemble components or install major parts. Likewise, they have to know what to look for on their workstations insofar as anti-virus programs running, or what they should do if they are alerted that their computer has a virus. A very important item that the user should be aware of, particularly if they are remotely located field users with little or no readily available IT support is how to obtain routine patches and hotfixes for their computers.

A number of methods should be called into play to accomplish the goal of training end users. First, there should be a well written, well published security policy that is easy enough for all to understand and follow. Secondly, user training should be a part of the overall process of making security awareness a commonly presented set of ideas. For instance, the IT department could hold "brown bag" lunch sessions in which users are invited to hear topics related to use of anti-virus programs and anti Spyware programs – in such a way as to encourage their use on their home computers – and to help them understand why such tools are used and mandated in the business world. Certainly one very important area of user training is in fostering good security habits, such as locking their computer screen or logging out completely when leaving their

workstations unattended. Still other important areas involve teaching users good password security such as choosing good, strong passwords, and not leaving their passwords exposed where anyone can see them. For users who are remotely located without readily available IT support, extra training effort is usually required so that they can learn how to retrieve and install virus signature updates, critical OS and software patches, and other routine maintenance that may otherwise be automated if they were actually in the home office and connected to the corporate network.

Additional Security Strategies

From a fundamental standpoint, desktop computer security can be enhanced by simple planning. By looking analyzing the organization's current security posture and performing strategic planning to implement security measures, the organization can have a better grasp of what it is doing presently, and what can be done in the future to secure workstations. Becoming familiar with the current laws and compliance recommendations, such as those found in Sarbanes-Oxley, NIST/FIPS (for government organizations), and HIPAA (for health care organizations) will help to have a basis of what has to be done when assessing what the organization is currently doing.

Perhaps one of the biggest assets to computer security is in that many of the things mentioned in the sections above can be automated to a large degree. For instance, rather than the end user having to worry about where to obtain the latest virus signatures or OS patches, enterprise systems can be put in place to manage these items for them. A centralized antivirus management server can ensure that they are always up to date with the latest signatures, while also alerting a central administrator if there is a virus infection. This takes the burden off of the user of having to understand how to perform the updates or even how to interpret virus removal procedures.

Likewise, an automated patching system can ease the burden of having to go to the vendor's web site to obtain patches, and patching can be scheduled so as to minimize interruptions to work caused by rebooting systems.

Other ways to incorporate automation is to use enterprise level tools such as the ability to create computer and group policies through whichever enterprise directory structure s in place for the OS in use. For instance, Windows networks rely on Active Directory for computer and user management, whereas Novell environments rely on NDS or eDirectory. Security templates can be applied to workstations when the computer is imaged by the IT department, and can also be pushed to the user's machine through the directory system policies. Periodic vulnerability scans presents yet another automated discover tool to help identify where potential problems exist. The goal of achieving a secure workstation does not have to be a constant series of manual tasks performed by either the end user or the IT staff, but can rather be automated and effectively managed by technology.

Conclusion

Workstation security is important because the number of computers that an organization has represents the number of potential entries in to the corporate network. If a workstation can be compromised, then corporate data, and quite possibly other corporate IT assets can be compromised as well. This paper discussed three important aspects of workstation security: the OS itself, physical security, and the end-users themselves. While there are more methods and issues that should be addressed, the scope of this paper was to touch on the fundamental aspects of workstation security.

Patching the OS and keeping it up to date will protect against the majority of attacks that target these types of vulnerabilities. Keeping antivirus and anti Spyware programs up to date as

well are important for protecting workstations from attacks. Ensuring physical security of workstations, particularly laptop computers will help to minimize losses of assets and potentially sensitive data. Finally, user training was discussed as a measure to help users become more security aware so that they can contribute to security through knowledge rather than contribute to insecurity through lack of knowledge. Planning and risk management are also important aspects of computer security in that they allow an organization to see what it is presently doing (or not doing) to secure workstations. By implementing a these fundamental concepts, an organization can help strengthen its security posture and contribute to the overall IT security program.

References

- Bradley, Tony, (2005) *What is a Bot or Zombie?*, Downloaded from http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot_p.htm on November 1, 2005.
- Carnegie Mellon University, (2003), *Securing Desktop Workstations*, CERT Coordination Center, downloaded from <http://www.cert.org/security-improvement/modules/m04.html> on October 22, 2005.
- Holden, Greg, (2003), *Guide to Network Defense and Countermeasures*, Boston, MA: Thomson Course Technology
- Limos, Robert, (2004) *Plague Carriers: Most users unaware of PC infections*, CNET News.com, downloaded from: http://news.com.com/Plague+carriers+Most+users+unaware+of+PC+infections/2100-1029_3-5423306.html on November 2, 2005.
- McClure, Stuart, et al, (2005), *Hacking Exposed: Network Security Secrets and Solutions, Fifth Edition*, Emeryville, CA: McGraw-Hill
- Panko, Raymond R., (2004), *Corporate Computer and Network Security*, Upper Saddle River, NJ: Pearson Education, Inc.
- Tittel, Ed, (2003), *Policy for the Real World: Physical security*, downloaded from http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci891293.00.html on November 1, 2005.