Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Secure Computing - An Elementary Issue

This paper was developed as a resource for elementary school technical support personnel responsible for maintaining a safe and secure computing environment. It is meant to provide a context for, and overview of, security issues in elementary school computing. A case is made for developing security policies to protect equipment and data which expand the scope of the familiar Acceptable Use Policy. Common threats to secure computing are identified and steps for mitigation are discussed.

Copyright SANS Institute
Author Retains Full Rights

AD

Susan J. Briere – GIAC

Practical Assignment
Version 1.4

Secure Computing—An Elementary Issue

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Abstract

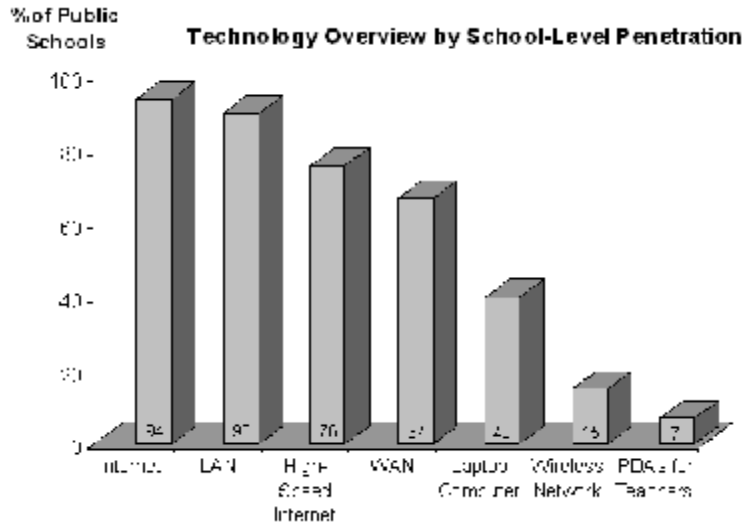
This paper was developed as a resource for elementary school technical support personnel responsible for maintaining a safe and secure computing environment. It is meant to provide a context for, and overview of, security issues in elementary school computing. A case is made for developing security policies to protect equipment and data which expand the scope of the familiar Acceptable Use Policy. Common threats to secure computing are identified and steps for mitigation are discussed.

Secure Computing

Elementary schools have embraced computers as an effective means of engaging students in the learning process. They serve the students' needs in a variety of ways. Students welcome computers as a tool for learning—as well as a fun choice at free-time. Adults marvel at how easily students interact with computers and how motivated they are to use them.

In support of this realization we've seen explosive growth of information technology in elementary schools. A combination of federal legislation and funding in support of increased access to technology has fueled this growth. Elementary schools now have networked computer labs, libraries, classrooms, administrative offices and special services. There are offerings for alternative types of computer-based instruction, such as distance learning and professional development on virtual campuses.

The Telecommunications Act of 1996 served to expand and maintain an existing system of universal service that provides schools and libraries with affordable access to advanced telecommunications.[1] As a result, the proportion of instructional classrooms with Internet access increased from 14% in 1996 to 77% in the year 2000, with about 98% of schools having some internet access.[2]



Market Data Retrieval's annual survey results of the current state of technology in U.S. schools demonstrate a variety of technologies in use.[3]

[1] U.S. DoE, -Rate Fact Sheet
[2] Digest of Education Statistics
[3] Technology in Education 2002

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

While elementary schools may not be in the business of generating revenue, they are held accountable for making sound investments in their educational facilities. In recent years Technology Literacy Challenge Funds and E-Rate discounts allowed schools to invest in new computers, peripherals, software, high-speed Internet access, networking equipment and infrastructure, as well as personnel to mentor the use of information technology. K-12 technology expenditures were expected to reach $8.8 billion by 2001-2002.[4]

For the first time, in many schools, new computers and networking equipment have been deployed en masse. This creates a need to provide adequate technical support for these installations. Elementary schools often struggle to afford technicians who have formal certification or IT-related degrees. It is common to find a part-time technician supporting a multi-platform LAN of servers, routers, switches and hubs with anywhere from 50 to 150 networked clients, the installed software and peripherals; printers, scanners, still and digital video cameras, and projection devices. The age of the equipment varies widely with a number of operating system implementations and software versions to match, further increasing the need for support.

Elementary schools strive to make these resources readily available to students, staff, faculty and, in many cases, community members. In a nurturing environment where openness and sharing is essential for learning, promoting a secure computing strategy may seem like an oxymoron. They do, however, understand the importance of providing a safe and secure environment for students while they pursue opportunities for learning. They also teach students to treat with respect learning tools such as the manipulatives, text books, workbooks and workstations typical to elementary education.

Computer networks present a new set of challenges to administrators and technical support personnel for providing a safe learning environment. Not so long ago the hot debate about network security in elementary schools was whether students should have password-protected accounts or whether the "cubby rule" sufficed. The cubby rule states, "You don't touch things in your neighbor's cubby" (and, by extension, you don't log into your neighbor's account on the network and mess with their files). Kindergarteners being introduced to computer lab rules nod their heads sagely when network security policy is presented in this context. They know the cubby rule.

Today, network security is a much bigger issue and the context is difficult to define. The dangers are real; they are physical, digital and intellectual, with threats that multiply and divide. The threats exist within and without, feeding off vulnerabilities that are inherent in the technology and the users. It is daunting for technical support personnel in elementary schools (who quite often have other professional responsibilities) to identify, quantify, and justify the measures necessary to maintain a safe and secure network installation.

A Network Security Policy defines the school's expectations for proper computer and network use and defines procedures to prevent and respond to security incidents. The goal of the policy, written clearly and concisely, is to balance the availability of resources with the need for protection. The policy describes what is covered, defines contacts and responsibilities, and outlines how violations will be handled.

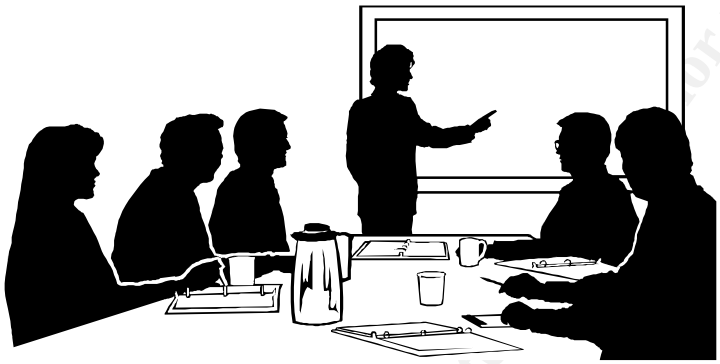
[4] Cisco's Commitment to Education

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

In A Short Primer for Developing Security Policies,[5] Michele D. Guel suggests that smaller documents are easier to maintain and update. She identifies some key policies, appropriate for elementary school computing environments, that can be created as separate documents:

- Acceptable use
- Baseline host/device security
- Remote access
- Information protection
- Perimeter security

The security policy should be developed by a group of stakeholders who represent the school community. Many schools have active Technology Committees that serve to provide oversight and direction. These committees, made up of administrators, school directors, technical support personnel, educational technologists, classroom instructors, staff, and community members develop policy and present it to school boards for adoption.



The process of developing guidelines for secure computing includes defining:

- what needs to be protected
- what threats exist
- the likelihood of the threat becoming reality—risk assessment
- what measures are needed to protect the school's assets in a cost-effective manner
- how to review and improve the oversight process

➢ What are you protecting? What are the assets in school computing?

- *Student records*
- *User files and documents*
- *Student access to appropriate material on the internet*
- *Computer equipment and peripherals*
- *Software applications*
- *Server/network/workstation configurations*

[5] Guel, P.11

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- <u>What are the threats</u>

-Student Records

- disclosure of confidential information (FERPA)
- falsification of records
- theft of information

-User documents

- invasion of privacy
- sabotage
- theft

-Student access to appropriate materials

- unfiltered Internet content
- non-compliance with CIPA or COPPA
- loss of e-rate discounts as a result of non-compliance

-Hardware - computer equipment and peripherals

-Man-made Threats

- abuse of equipment
- use of unnecessary force
- food or drink spills
- theft

Natural Threats

- lightning, power surges/sags
- high temperature/humidity
- dust/dirt
- rain/water damage
- fire
- severe weather; flood, hurricane, tornado

-Software – licensing and media

- licensing misuse
- application Piracy
- theft of media
- unauthorized installations
- unauthorized downloads
- downloading viruses
- introducing viruses via media from home

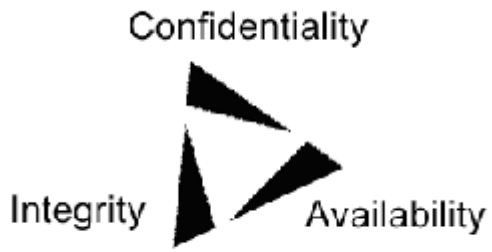
-Sever/Network/Client Workstation Configurations

- unauthorized access to the network
- unsecure operating systems
- unprotected passwords
- unprotected shares
- internal attacks
- external attacks

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

➢ Risk Assessment

Physical threats to equipment can be easy to identify yet remediation may be difficult. Making resources available while balancing the need for protection requires a focused look at what the school is required to deliver in terms of information technology. How does the availability or integrity of data resources affect planned outcomes with regard to



- Student performance
- Learning portfolios
- Instructional quality
- Ability of administration to meet state and federal reporting guideline

How important is it to protect the data your school generates? In the context of information security, threats are defined as activity that may compromise the confidentiality, integrity or availability[6] of the school's data assets.

Student Records

According to the Family Educational Rights and Privacy Act (FERPA), schools must have written permission from the parent or eligible student in order to release any information from a student's education record. “Education records” are broadly defined as: those records, files, documents, and other materials, which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution. 20 U.S.C. §1232g(a)(4)(A). (See also 34 CFR §99.3.)[7] FERPA applies to all agencies and institutions that receive federal funds including elementary and secondary schools, colleges, and universities. The combined need to ensure the integrity of the data for reporting purposes with the need for protecting confidentiality and availability of the data makes having an information protection policy a necessity.

User Documents,

Unauthorized access to documents stored on a school network constitutes an invasion of privacy. Harkening back to the "cubby rule" students may assume that the documents stored in their digital cubby are not available to unauthorized users on the network. While password protection is a viable option as students get older, the culture of maintaining a secure password is not pervasive. A clearly defined acceptable use policy signed by students, and parents in some cases, educates network users about expected behavior and the consequences of violating policy.

Student Access to Appropriate Materials

Approximately seven thousand new sites are added each week to the Internet. Teaching students to navigate the Internet safely and effectively is important for maintaining a safe computing environment. Trojans lay in wait on compromised websites for unsuspecting users. Downloading a program that seems harmless and fun can introduce a vulnerability

[6] Network Security, p.1-5
[7] US Dept of Education, 34 CFR Part 99

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

to the network allowing unauthorized access, and control over, network resources. Recent legislation, the Children's Internet Protection Act (CIPA), requires schools that receive E-rate discounts on Internet service and internal connections to have an Internet Safety Policy and to filter out access to inappropriate content on the Internet. The Internet Safety Policy also must address "the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications", as well as "unauthorized access, including hacking, and other unlawful activities by minors online".[8] Most schools could improve network security by incorporating an Internet Safety Policy whether they receive E-rate or not.

Computer Equipment and Peripherals

Man-made Threats to Equipment

In 2000 the average public school contained 110 computers.[9] Physical threats to the equipment can be significant and costly if acceptable use has not been defined. In spite of ample evidence of the popularity of computers with students the potential for a user to become frustrated when the program or equipment isn't responding in the expected manner is not uncommon. This frustration can result in the abuse of equipment and/or the use of unnecessary force.

Enforcing a security policy that clearly defines the expectations of acceptable use and the consequences of misuse mitigates this threat. An example of a no-cost measure to remove the threat of damage from liquid or food spills is not allowing food or drinks near computer equipment. Reinforce this by posting a reminder near equipment which clearly defines the policy and consequences of violating the policy.

Clearly marked or labeled equipment and media can deter theft. (One exception to this is servers and other networking hardware. While it is still important to identify equipment it is not good practice to display machine names or IP addresses in plain view.) The smaller the device, the easier it will be for it to disappear. Memory cards and sticks used in digital cameras, as well as the cameras themselves are so compact in size they require close monitoring. Signout sheets that identify who is responsible for the equipment should be required by policy and will provide accountability when tracking down missing items. Keeping an inventory of computer equipment, peripherals and software licenses provides accountability for what should be where and how many of them should be there. A security policy should identify intervals for monitoring and updating hardware and software inventories and who is responsible for maintaining the inventories.

Elementary schools want to make their educational resources readily accessible. It is possible to respect this practice and still maintain a healthy environment for expensive networking equipment and cabling installations. A secure, *as in locked*, area is necessary for network servers, patch panels, switches and routers. A security policy identifies who is responsible for the equipment and who has access to the secured areas.

[8] Children's Internet Protection Act, Section 254(I)
[9] Digest of Education Statistics, 2001

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Natural Threats to Equipment

A security policy describes what measures are taken to protect sensitive equipment from natural threats. Servers and network hardware need to be protected from potential damage by lightning, power surges and prolonged power sags. An uninterruptible power supply (UPS) guards against the hazards of unconditioned power. Another benefit is that most UPS manufacturers include software that can be configured to automatically shut down programs and equipment in an extended power outage.

Electronic equipment is vulnerable to damage from overheating. The inside of a CPU case is up to 40° F higher than the external air temperature. High temperature combined with a layer of dust acting to insulate the electrical components will result in equipment failure. A baseline host/device policy defines the schedule for equipment cleaning and maintenance as well as who is responsible for performing the maintenance.

Low-cost items like fire extinguishers, surge protectors and uninterruptible power supplies, and locating equipment high enough to avoid minor flooding are simple measures to implement. These measures can be part of the information security policy document or the baseline host/device security policy document.

Assessing the risk of severe weather—floods, tornadoes, and earthquakes, will generate different outcomes depending on where you are located. In an area prone to severe weather conditions there may be a policy already in place to address facility vulnerabilities. Become familiar with the terms of the school's insurance coverage with respect to computer equipment. Use existing plans and make modifications for your specific needs.

Backing up Data

An information protection policy for your data assets includes having a backup routine. Defining the type of backup you use, how often to backup the data and where the backups are stored are a part of the policy. There are many ways to backup data. The main difference in the way data is backed up is the device and the media used to store the data.

Tape backup units are relatively inexpensive, for the unit and on a per-gigabyte basis for the media. They tend to be slow, however, and the media has a limited shelf life. Removable storage drives, such as Zip drives and Jazz drives are an inexpensive option where smaller amounts of data are being backed up. Removable hard drives can handle much larger amounts of data as well as offer fast access rates with good reliability.

RAID storage (Redundant Array of Inexpensive Disks) offers a range of performance and reliability capabilities. A simple form of RAID storage, called mirroring, writes data to two separate disks simultaneously. If one disk fails the other retains the data intact. More expensive methods of RAID storage use more disks and stripe the data across multiple volumes using an algorithm to recover lost data should one of the disks fail.

Commercial backup services over the internet encrypt the data, compress it, and then send it over a high-speed, secure web tunnel to their backup servers. Keeping a copy of the backup media offsite is protection in the event the building sustains damage or in case the local copy becomes unusable.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

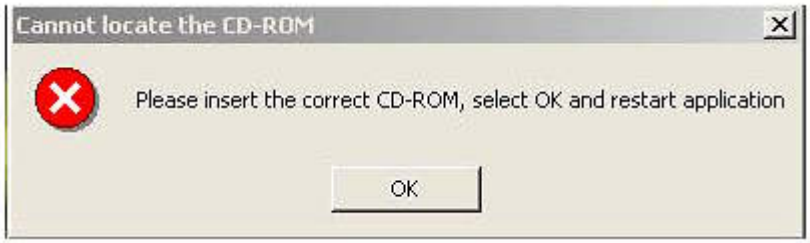
Software Licensing Abuse and Piracy, Media Theft

Software licensing controls authorized use of a program. Elementary schools acquire software in many ways, including planned purchases, classroom teacher purchases, donations, downloaded programs and plug-ins, and the odd software programs that trickle in from home. Not all of these methods are O.K. In fact, the trend is toward planned purchases at the district level. The main reason for this shift is the threat of litigation for software piracy. The following excerpt from an article in *eSchool News Online* underscores the importance of compliance:

> In a case that might serve as a warning for district administrators and technology coordinators from coast to coast, a school system outside of Chicago has agreed to pay $50,000 to a computer trade organization after discovering that a former employee had copied software onto school computers illegally.[10]

Compliance with software licensing is important for several reasons; it's ethical, helps keep the cost of legitimate software down, allows schools to have accurate inventories, provides schools information about which software titles are most in demand, reduces the risk of infected media being used, and it eliminates the possible cost of litigation.

Many schools are choosing to support an approved list of software titles. This reduces the amount of technical support required to support the idiosyncrasies of applications and provides a consistent set of tools for learning. Unauthorized installations, *even with proper licensing*, can be costly to support. Another point to consider, one that is increasingly important, is the number of security patches issued by software authors on a regular basis… if you don't know what you have installed you won't be effective in keeping it patched.



Many educational programs will not execute unless the CD is in the CD-ROM drive. This introduces several vulnerabilities with respect to the software media. CDs must be stored in proximity to where they will be used. The time it takes to distribute, load, unload and store the CDs in a lab environment makes it easy to lose track of the media. Classrooms with computers need their own copies of the CD handy. It also requires the media to be handled repeatedly during use, which in a K-6 environment may reduce the life of the media considerably. Decrease risk by identifying who is responsible for program media in each situation.

Define how media is labeled, stored and handled. Some schools purchase CD towers which can make several CDs available at once over the network. This approach has caveats, not the least of which is running applications over the network that were not designed for that purpose. Performance can be quite slow and clunky. There is also additional support required for the CD tower.

[10] eSchool News Online, Sept 21, 2001

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Threat of Viruses

On July 19, 2001 more than 359,000 computers were infected with the Code-Red (CRv2) worm in less than 14 hours. At the peak of the infection frenzy, more than 2,000 new hosts were infected each minute. 43% of all infected hosts were in the United States.[11]

Elementary schools are typically not in session during the summer months. Consequently, many do not contract technical support on a year-round basis. In his analysis of the spread of the Code-Red virus, author David Moore concludes,

> This assault also demonstrates that machines operated by home users or small businesses (hosts less likely to be maintained by a professional sysadmin) are integral to the robustness of the global Internet. As is the case with biologically active pathogens, vulnerable hosts can and do put everyone at risk, regardless of the significance of their role in the population.[12]

His remarks apply particularly well to elementary schools because they may have a live network without an active system administrator for certain periods of the year.

The cost of computer viruses to elementary schools is accounted for most directly in labor costs to clean the virus from individual machines, restore from backup, reinstall or reconfigure affected software and, less directly yet importantly, in loss of access to educational resources for the school community.

Viruses pose a threat on multiple fronts. Assessing the risk posed by the various types of viruses includes questions such as

- do we allow diskettes from external sources
- who uses email and what training do they receive
- do we allow users to download and run programs from the Internet
- do we control access to the websites users visit
- do we use applications that are susceptible to macro viruses
- do we have unpatched computers vulnerable to external attacks

Once the risks are identified a security policy defines steps to avoid contracting a virus, as well as methods for containment and cleansing in the event of infection. Use the policy to define the scope of the virus protection provided; roles and responsibilities for installation and monitoring of antivirus software, including a schedule for updating virus definitions.

- where is anti-virus software installed
- who is responsible for updating it and how often
- how often does training take place for end-users
- how is critical information disseminated when you're under attack
- what steps are taken to contain an outbreak
- what services are affected in the event of an outbreak

[11, 12] The Spread of the Code-Red Worm (CRv2)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Server/Client Configuration Vulnerabilities

The client-server architecture is built around network clients requesting access to the server's resources. It is important to define who needs access to what resources and use a policy to restrict unnecessary access. The goal, again, is to serve and protect—provide users with the resources they need without creating or exposing system vulnerabilities.

Unauthorized network access
Internal attack

A dangerous assumption for a system administrator to make is that their brand new server came out of the box configured for security. It is more likely the server was configured for ease of use. It *is* called a server and it was purchased to provide network services to its clients. The degree of vulnerability depends on the Network Operating System (NOS) and any pre-purchase configuration arrangements that were made. The same logic applies when deploying client operating systems.

As an example, Windows98 was never designed to be a secure operating system. It was designed to integrate easily with a broad range of application software and peripheral devices. WindowsNT, conversely, was designed for central administration of security and was not as popular from a compatibility standpoint.

This, and a lack of educational programs ported to WindowsNT has led to large installed base of Windows98 computers. The security implementation in Windows98 is largely based on security by obfuscation. Its security policies are easily compromised and vulnerabilities exposed. Elementary schools planning new Microsoft purchases will choose between Windows2000 Professional and WindowsXP Professional; both featuring centralized management of security. Early reviews suggest that WindowsXP Professional, the successor to Windows2000 Professional, offers improvements in the management and administration of the desktop, as well as the ability to play nicely with peripherals.

Because of the popularity of the Microsoft operating system there is a great deal of energy focused on breaking it. Hackers uncover new vulnerabilities almost daily, which may be a threat to the school network. Mailing lists such as Microsoft's Security Bulletins include information on necessary patches and updates for your network configuration.

While conducting the risk assessment there is an opportunity to discuss the benefits of providing users with a consistent interface (controlling the desktop and access to resources on the local machine). The main objective in the elementary school computer lab and classroom is to get the users to the tools and resources they use as neatly as possible. A baseline host/device security policy defines how new equipment is set up and configured prior to joining the network and becoming available for use:

- How are we integrating computers in our curriculum
- What tools are we making available to support learning
- How do students access these tools
- What other resources do students need access to
- What vulnerabilities do we expose and how do we protect them

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Password protection

A security-minded operating system is a good starting point. Building a security-minded user base is equally important for network security measures to be effective. Passwords are commonly identified as a weak link in the security chain. According to SANS Security Essentials the security policy should specify procedures for creating passwords. These may include a minimum password length of 8 characters including a non A-Z character.[13] Correctly formulating a password will not ensure the security of the password if it is stored on a sticky note under the keyboard. The committee conducting the risk assessment and developing the security policy will need to define appropriate consequences to encourage users to maintain password security.

Open network shares

Central to the client/server schema is sharing information located on the network with users who need it. Access to shares can be restricted by using access control lists. This requires users to authenticate before access to a share is granted. Unprotected network shares make data stored on that share vulnerable to theft, corruption or virus infection. Propagation of the W32/Sircam worm via open network shares required no human intervention. W32/Sircam had the potential to create breaches of confidentiality due to the virus' ability to mail sensitive information, denial of service by creating a file known to consume all free space on the C: drive, or self-propagate via mass e-mailings. W32/Sircam was soon followed by the Nimda virus and more recently, the same type of blended threat has presented itself in the Bugbear worm.

Network shares configured for remote access are often targeted by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Windows machines have been used as intermediaries in various types of denial of service attacks for years. Elementary school networks that are not adequately secured can be compromised and used as a launch pad for attacks against other computers as was highlighted by a recent distributed denial of service (DDOS) attack launched against the 13 root servers for the Internet's Domain Name System.

Auditing *Network* Activity

Who's doing what on the network? Windows and Unix servers have logging features that make auditing network activity more manageable. Audit events fall into two categories, success events and failure events. A success event is logged when a user has successfully gained access to a resource, whereas a failure event shows that they tried, but failed. Often, the pattern of events is as important as the events themselves. For example, a series of failures followed by a success may indicate an attempted attack that was eventually successful.[14] This critical feature won't help if passwords aren't properly protected. The integrity of the audited information—what's being accessed

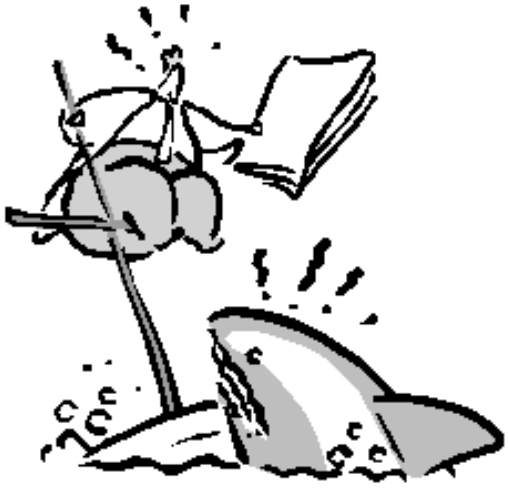
[13] Network Security p. 2-18A
[14] Microsoft TechNet

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

when and by whom—is compromised when a password can be retrieved from the underside of the keyboard or left in the open in an unlocked drawer without consequence. Recent estimates claim that unauthorized access and the subsequent damage to data is traced to internal sources in as many as 80 percent of cases.

External Attack – Guarding the Perimeter

External attacks take many forms, from automated attacks that exploit CGI vulnerabilities and web application weaknesses to running vulnerability scanners that identify open doors; from passwords crackers and spoofing user IDs to denial of service attacks that render network resources inaccessible. These tools increase in sophistication with each new version and are readily available for download on the Internet. The level of skill required to successfully implement these tools is considered negligible. Preparing a defense includes using many of these same tools to evaluate your state of security.



Vulnerability scanning is "the automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened."[15] Tool or weapon? That depends on who is running the application. A sysadmin uses vulnerability scanning to identify weaknesses in order to direct security efforts where they are needed most. (Intrusion detection systems, mentioned below, address the other half of that equation.) These application scanners generally contain a database of known security exploits and test for vulnerability to them. This requires the database to be updated periodically as new exploits are identified, limiting their effectiveness to known weaknesses.

The recent attack on the Internet's root servers most likely used automated tools placed on unsecure (and unknowing) computer networks, according to an interview on National Public Radio with Paul Vixie, Chairman of Internet Software Consortium Inc. In a Washington Post article Alan Paller, research director at the SANS Institute said,

> "The only way to stop such attacks is to fix the vulnerabilities on the machines that ultimately get taken over and used to launch them." [16]

Many security organizations are concerned that these attacks will become more frequent and gain intensity. In September, 2002 the White House issued a draft of the National Strategy to Secure Cyberspace. The draft outlines involvement by home

[15] Webopedia
[16] McGuire, Krebs

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

owners, small businesses and universities, as well as internet service providers, state and federal agencies and large corporations to take measures to secure U.S. information systems against deliberate and malicious disruption, in support of the National Strategy for Homeland Security and the National Security Strategy of the United States. Elementary schools have a responsibility here, as well, to provide secure resources. There are many ways to reduce the risk of an external attack.

Traditionally, a firewall is a wall separating two areas, in a building, a car, etc., to prevent fire from propagating from one area to another. By extension, the term is used for equipment that is used to separate two networks, to prevent hostile packets from one network from reaching the other. The most common firewall configuration protects an organization's private network from the Internet.[17] A firewall may employ network address translation (NAT), proxy services or stateful packet inspection. NAT allows a LAN using a private IP address range that does not route to the Internet to use one public IP address for all outgoing connections and prevents most incoming connections. Proxies are mostly used to control, or monitor, outbound traffic. Some application proxies cache the requested data. Caching of frequently accessed data has the added benefit of reducing the bandwith requirements of the Internet connection and improves access speed. A stateful firewall inspects all packets going through the firewall. Packets are only forwarded if they match the access control list. It is called “stateful” because the firewall can permit outgoing sessions while denying incoming sessions. Stateful firewalls with complex access control lists may produce latency issues which can slow network traffic. Choosing and using a firewall is a very basic security measure for any network with an Internet connection.

Intrusion detection systems (IDS) provide visibility of network threats by attempting to detect an intruder breaking into your system or a legitimate user misusing system resources. They capture and report attempts to exploit known vulnerabilities, as well as detect activities that are not typical of normal network behavior such as reconnaissance activities used for information gathering, port scanning for 'open doors' and packet flooding used in a denial of service of attack.

Putting it All Together, Defense in Depth – A Logical Conclusion

Address threats to the computing environment by developing meaningful policies. Define your school's mission in terms of information technology; what resources are you committed to providing to students, faculty, staff and administration, to the extended community and beyond? Define the policy(ies) to protect those resources. Is the intent of your Internet connectivity to provide users with access to information on the web or does it include offering services such as web hosting, email hosting or distance learning? How does this increase the number of threats to your network and the cost of securing the resources? Accessing information and offering access to information are two very different security domains. Providing external access to resources on your network requires the risk assessment to address additional threats. Are the most compelling risks to the school's computer systems internal threats? The security measures implemented by your policies should identify the threats, provide early

[17] CSE 127: Introduction to Computer Security

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

warning of system weaknesses and allow adequate time to detect and respond to an impending threat. Define acceptable use of the resources and provide a detailed description of responsibilities and methods for accountability. Communicate the policy to users. Enforce the policy.

In conclusion, defense in depth is a philosophy for secure computing. This philosophy recognizes the existence of credible threats to your computing environment and places multiple barriers between an attacker and vulnerable resources. Those resources—the physical plant (equipment and infrastructure in your installation), the network resources, and the digital assets generated and stored within your organization each have vulnerabilities. Keep operating systems patched, require authentication for access to network resources, install virus protection, monitor traffic in and out of the network and keep a back up of all critical data. Above all, keep in mind that security is an elementary issue.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

[1] U.S. DoE, Discounted Telecommunications Services for School & Libraries, E-Rate Fact Sheet URL: http://www.ed.gov/Technology/comm-mit.html

[2] Digest of Education Statistics, 2001, URL: http://nces.ed.gov/pubs2002/digest2001/ch7.asp

[3] Technology in Education 2002, URL: www.schooldata.com/publications3.html

[4] Cisco's Commitment to Education, K-12 Education Market Background URL: http://www.cisco.com/warp/public/779/edu/commitment/edu_internet_economy/k12_market.html

[5] Guel, Michele Dl "A Short Primer for Developing Security Policies" Copyright 2001 p.11 URL: http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf

[6] Volume 1.2, SANS Security Essentials II: Network Security, p.1-5

[7] US Dept of Education, Family Educational Rights and Privacy Act, 34 CFR Part 99 URL: http://www.ed.gov/offices/OM/fpco/ferpa/ferparegs.html

[8] Children's Internet Protection Act (CIPA), Section 254(I) URL: http://www.sl.universalservice.org/reference/CIPA.asp

[9] Digest of Education Statistics, 2001 URL: http://nces.ed.gov/pubs2002/digest2001/ch7.asp

[10] Guerarde, Elizabeth B. "District's $50K 'Piracy' Settlement Leads to Policy Changes" eSchool News Online, Sept 21, 2001 URL: http://www.eschoolnews.com/news/showStory.cfm?ArticleID=3028&ref=wo

[11, 12] Moore, David "The Spread of the Code-Red Worm (CRv2), June 14, 2002 URL: http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml

[13] SANS Security Essentials II: Network Security text book, p. 2-18A

[14] Microsoft TechNet, Windows2000 Security, Chapter 6 – Auditing and Intrusion Detection URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/windows/windows2000/staysecure/secops06.asp

[15] Webopedia URL: http://www.webopedia.com/TERM/V/vulnerability_scanning.html

[16] McGuire, David and Krebs, Brian "Attack on the Internet Called Largest Ever" WashingtonPost.com, October 22, 2002 URL: http://www.washingtonpost.com/wp-dyn/articles/A828-2002Oct22.html

[17] Cryptology and Security Group, UCSD "CSE 127: Introduction to Computer Security" URL: http://philby.ucsd.edu/~bsy/Courses/cse127.w02/lec17/

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Additional resources

Marshall Brain's HowStuffWorks
How Computer Viruses Work
http://www.howstuffworks.com/virus.htm

CERT Coordination Center, Software Engineering Institute, Carnegie Mellon
A center of Internet security expertise
http://www.cert.org/

Microsoft TechNet's Security homepage
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp

Subscription page for Microsoft's Security Notification Service
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

SANS (System Administration, Networking, and Security) Institute Resources
http://www.sans.org/newlook/resources/

Network Security Library
http://secinf.net/

Security Software
http://www.ja.net/CERT/JANET-CERT/software/

GCK's Security-related URLs
http://www.garykessler.net/library/securityurl.html

Internet/Network Security
http://netsecurity.about.com/mbody.htm

American Libraries Association
Learn to Use the Internet as a Curriculum Resource – Elementary Curriculum
http://www.ala.org/ICONN/coursedes.html#elemcurr

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced