ED 457 215	TM 033 313
AUTHOR	Shermis, Mark D.; Averitt, Jason
TITLE	Security for Web-Based Tests.
PUB DATE	2001-04-00
NOTE	27p.; Paper presented at the Annual Meeting of the American Educational Research Association (Seattle, WA, April 10-14, 2001). Some text may not reproduce well.
PUB TYPE	Guides - Non-Classroom (055) -- Speeches/Meeting Papers (150)
EDRS PRICE	MF01/PC02 Plus Postage.
DESCRIPTORS	Computer Assisted Testing; Computer Security; Performance Based Assessment; Testing Problems; *World Wide Web
IDENTIFIERS	*Test Security

ABSTRACT

The purpose of this paper is to enumerate a series of security steps that might be taken by those researchers or organizations that are contemplating Web-based tests and performance assessments. From a security viewpoint, much of what goes on with Web-based transactions is similar to other general computer activity, but the recommendations here focus on what can be done to avoid the loss, compromising, or modification of data collected by or stored through the Internet. Among the security actions discussed are: (1) recovering from disasters; (2) development of security policies; (3) user-end security; (4) security for menu systems and control programs; (5) virus protection; (6) physical security; and (7) possible threats from the Internet. (Author/SLD)

Running Head: Internet Security

Security for Web-based Tests

Mark D. Shermis Jason Averitt

Indiana University Purdue University Indianapolis

This paper is prepared for the:
Annual Meeting of the American Educational Research Association in Seattle, WA
April 2001

Abstract

The purpose of this paper is to enumerate a series of security steps that might be taken by those researchers or organizations that are contemplating web-based tests and performance assessments. From a security viewpoint, much of what goes on with web-based transactions is similar to other general computer activity, but the recommendations here focus on what can be done to avoid the loss, compromising, or modification of data collected by or stored through the Internet.

Introduction

Several testing companies have now released tests for administration over the World Wide Web (the web) or are well into the process of doing so. While computerized testing has been in place for almost a decade, the use of the web as an administration format is relatively new (Shermis et al., 1997). The advantages of using the web as an administrative format are numerous, including: global reach, standard interface, immediate updating, centralized control, and ease of use. For testing purposes alone, web-based assessment allows subjects to work at a faster pace than with paper-and-pencil tests, and provides them with immediate feedback. Standardized tests can be administered at several locations while data are compiled at one central location. These advantages are often weighed against two significant drawbacks: inconsistent connectivity and a proneness to security risks. The former problem can be ameliorated with some technical measures, utilized by a systems administrator. The remainder of this paper is devoted to discussing the possible data collection risks for computerized testing and safeguards against those risks, with a special emphasis on the web-based format.

Where to Begin?

> The overwhelming attacks this week against some of the Internet's biggest companies required dozens of powerful "zombie" computers collectively aiming a crippling tide of data at target Web sites. Experts believe the hackers earlier had infiltrated and secretly installed their attack software on these computers, setting them up as unwitting accomplices in a crime-in-the-making. Were the operators of these computers merely victims of these unprecedented assaults, or were they partly to blame? It's a question with enormous consequences for the Internet, the sprawling worldwide network that has few rules and where security can range from ironclad to nonexistent. As the Internet's importance grows as an engine for America's economy, some experts wonder whether unsafe computers can continue to be tolerated, or whether there is any alternative. (Bridis, 2000)

This snippet, taken from an Associated Press Technology release, summarizes a recent breach in Internet security that paralyzed a number of U.S. commercial firms for a span of two days. This intrusion occurred on networks in the commercial arena, but intruders have also explored and destroyed systems maintained by government and educational institutions. If systems set up for academic purposes are not equipped to handle these types of events, then they are extremely vulnerable to intrusion. Although monetary gain is not a likely reason for an attack on academic networks, the desire to create general mischief should not be overlooked.

As is discussed later in this paper, most of what can go wrong with Internet data collection is common to many other types of computer transactions—power loss, virus infection and the like. There are processes which are specific to the Internet, and what follows is a brief description of the rare occurrence of outside intruders trying to gain access to a web-based data collection server.

The first step an outside intruder will use to gain access to a site is called “footprinting”. Footprinting is the creation of a profile or map of an organizations’ system and vulnerabilities using a fairly systematic method of examination. Hackers frequently use a variety of techniques to compile information regarding organization sources such as the Internet, extranet, intranet and remote access. The first phase of footprinting involves determining the limits of what is to be examined. For example, footprinting an entire organization is very different from footprinting only specific parts of the organization. Next, the hacker will perform an open source search, usually by checking the organization’s official web page. Several key pieces of information can be determined simply from examining the site. Such information can include: links to other servers related to the organization, actual security policies describing the security measures used by the organization, or any other information related to the target group. Hackers can also gain important information (e.g., who the system administrator might be) by employing various query types. The four main types that are typically accessed are organizational, domain, network and point of contact (POC) queries. These queries display information on the organization, the specific domain, the specific network, or administrative person, respectively. Potential intruders can also view the domain name server (DNS), a database containing IP addresses and their matching host names (McClure, Scambray, & Kurtz, 1999). Firewalls are typically used to prevent extensive footprinting by unauthorized users. It is also recommended that intrusion detection be used in addition, to log any attempts to footprint the organization's system. VisualRoute™ is a program that allows you to query the connections and routing for a particular domain. It will also permit you to collect network and domain information.

Once the key information of an organization has been discovered, the intruder will attempt to determine if this information is exploitable. Two common methods of this type of scan are Ping sweeps and Port scanning. Ping sweeps consist of sending echo packets to those IP addresses that have been detected during the footprinting process. The "pings" will report back to the intruder, telling whether the IP address is in use and available for attack. Since ping sweeps often precede an attack, it is crucial to detect these attempts as soon as they occur. Ping detection programs such as Network Flight Recorder (NFR) can detect the origin of the ping sweep and help determine whether an attack is about to occur. Steps can then be taken by the system administrator to secure those areas where the sweeps were reported.

Once these vulnerable systems have been identified, the process of port scanning can take place. This is when the open ports of a system are scanned to determine what type of operating system is in place and what kind of applications are being used. This helps the intruder to decide which methods to use, since different systems and applications have different vulnerabilities that intruders will use to infiltrate the system. Once open ports are infiltrated, intruders can mask their origin, take up disk space, attempt to bypass firewalls, and further compromise the system (McClure, Scambray, & Kurtz, 1999). The more ports that are in "listening" mode, or in use, the more vulnerable the system is to infiltration. Like detection of ping sweeps, detection of port scanning attempts is an important preventative measure to determine from where and when an attack may occur. Some programs can scan an IP subnet and show what devices are responding on that subnet. Each of the responding devices is then queried via the Simple Network Management Protocol (SNMP), which helps administrators manage their networks. Additional details about each device can then be displayed as well.

Once an intruder has identified the weak points in the system, these spots will likely be used as access points to the network. These points can be identified by successful footprinting techniques or by successful port scans. These open ports then provide an open door for the intruder. After the network has been accessed, the goal of the intruder is to gain access to the machine of the system administrator. This will give the intruder full access to the entire network. One of the key mechanisms to accomplish this is to exploit vulnerabilities in password administration. If, for example, an administrator or employee leaves passwords on the default setting, the system can be accessed with relative ease. Intruders who are simply familiar with the organization's software can crack these generic passwords. This type of mistake is attributable to either ignorance of the importance of secure passwords (usually on the part of the average employee) or laziness and can be corrected simply by supplying all members of an organization with information regarding their accounts and passwords. Even if strong passwords are used, the system is still in potential danger. The intruder may install a keystroke logger on at a remote location within the system. After waiting for a short period of time, the network IDs and passwords of various individuals can be logged by the intruder. The information gained allows the hacker to access more machines in the system via hidden Trojan programs until he or she finds an entry by the system administrator. After the system administrator's password is discovered, the intruder gains access to the entire system.

Other Considerations

There are probably no "fool-proof" security systems that will protect one against every possible mechanism that would compromise, corrupt, or destroy data collected via the World Wide Web. Given the fact that a computer could fail at any possible moment, there will always be some risk involved. However, there are preventative measures that can be taken against most types of problems.

Before any trouble occurs one might wish to engage in a risk analysis. The process involves examining the computer system for information that needs to be protected, and whether that information is subject to a possible security threat. This will help to determine where trouble is most likely to occur by pinpointing weak spots in the system. By performing this simple procedure, valuable time can be saved when attempting to restore lost information or functions. This relatively simple policy can be used to protect against the loss or compromise of data such as test banks, subject identification, and other confidential or otherwise important information.

There are three relatively simple steps involved in performing this analysis (Brandt, 1998). The first is determining precisely which components are security risks. All applications and data should be inventoried to establish a record of the present components. If the system is very large, an inventory management system can be used to keep track of the system components. Software such as the Zero Administration Client (ZAC), by McAfee, is a useful alternative for the management of a large system.

The second step is to examine the concrete ways in which threats could occur. Examine each component individually to identify specific problem possibilities. Examples of these possibilities include not only software failure, but power loss, hardware failures, and tampering and hacking.

The final step is to develop recommendations for solutions to each possible threat to every component. By systematically generating solutions to each problem examined in the second step, one can generate a checklist of procedures that can be easily accessed and followed in times of emergency (Benson, 1998b). For example, in developing a risk analysis for ping sweeps, one would go through the following process: identify areas of the system most likely to be affected (an active, unmonitored IP address used by the system), identify the specific processes that could be used by an intruder to exploit these points (sending programs to find these addresses), and come up with countermeasures to deal with these processes (such as software to detect this activity).

A number of security actions should be taken to insure the safety and well being of the organization's network. The situations and areas that should be accounted for are: recovering from disasters, the development of security policies, user-end security, security for menu systems and control programs, virus protection, physical security and possible threats from the Internet. While most of the headlines regarding data loss or compromise have focused on external threats, it is more likely that if you have a problem, it will stem from the problems listed immediately above. Far more data is lost because someone didn't back up a file than from a malicious hacker snooping for open ports in your network.

When a situation occurs that results in the loss of information or applications, recovery can be made easier if a contingency plan has been developed beforehand. By deciding what actions to take prior to the emergency, the process of recovery will be easier and less stressful. The back up plan should explicitly outline which actions are to be performed, the situation that should precede these actions and the actual person responsible for carrying out the actions. The best choice for this person would be the system administrator or the employee with the most knowledge of the system. If this is not possible, then someone should be specifically trained for these particular situations.

Next, the organization should work toward developing effective security policies. Developing a policy differs from company standards and procedures. Standards and procedures describe exactly how the policy is to be carried out. A good policy will simply be an overall approach to insuring the security of the system, specifying which parts of that system are to be secured. The policy is made up of four parts: the purpose, the scope, general policy statements and policy standards (Benson, 1998b). The purpose describes what the policy is intended to accomplish. The scope tells who and what will be subject to obey the policy. General policy statements are the rules by which the policy is put into place. These rules should indicate the people and positions responsible for certain tasks, define the use and misuse of the computer system, who will receive access to the system, which parts of the system need to be protected, and the consequences of violating the policy. An example of a policy statement would be something similar to, "Network IDs for Department X will be given out by the system administrator only, unauthorized personnel providing IDs will be reprimanded". Lastly, policy standards should be stated, in which the tasks necessary to support the policy statements are listed.

It is only with a modest sense of irony we point out that perhaps the easiest way to lose computerized test data is for someone to walk into a testing facility and physically remove a computer or hard disk. By treating the testing facility as one would treat any space containing confidential information, this simple type of intrusion can be easily avoided.

If a PC is to be accessed by outside or multiple users, "front-end" security should be established. This is accomplished by securing menu systems that provide access to the control programs. These programs in turn, provide entrée to files and applications that must be protected. By restricting access to these programs, the organization reduces the risk of damage to important files and applications due to the actions of users not familiar with the network.

Along the same lines as installing front-end security, securing menu systems involves disabling some "user-friendly" options that are designed to provide easy access to all parts of the system. An example of the type of option to be eliminated is the CTRL+ALT+DEL function, which automatically shuts down and reboots the machine. By disabling features like this, the administrator reduces the amount of interference to the original set-up of the system. Eliminating the Prt Scrn (print screen) button on some computer keyboards also helps to reduce a change in the set-up, while keeping testing information from being printed by examinees or research subjects.

One of the most under-utilized and abused security features implemented in most computers has to do with password protection. Many computers have the option of requiring a password before allowing a computer to complete its boot-up process; nevertheless this feature is often disabled because it is considered an inconvenience. Even when passwords are required, many users will resort to easily guessable defaults (e.g., "guest", "admin", "user1") rather than implementing a secure alternative. Passwords should be at least 8 characters long, should consist of letter-number combinations, and should not appear among those that are commonly used. System administrators should be able to provide users with helpful tips on creating secure passwords. It should be noted that even good password systems can be compromised if the password information is not properly encrypted in the program that uses it. We discuss encryption later on in this paper.

The whole business of preventing external threats to your network ends up consisting of a number of incremental steps designed to thwart the attempts of others in a game of Internet "cat and mouse". One of the easiest ways to prevent external intrusions is by disconnecting from the Internet and simply running a local area network (Intranet). Combined with proctoring of the machines, a secure menu system, and attention to safety (backing up, emergency power supply, and anti-virus software), your system will be relatively secure.

However, if you must be connected to the Internet to perform web-based testing for example, there are some steps you can take to help secure your site. First, perform a computer security check-up. It is possible to have your system analyzed to determine the weaknesses for which it is vulnerable. For example, Shields UP! (https://grc.com/x/ne.dll?bh0bkyd2) can perform a basic analysis for Windows-based machines. After connecting to your network, this web site will return a full report on technical aspects of your communications setup such as the number of open ports and how stealthy your system is to outside intruders.

In addition to examining your Internet vulnerabilities, you can also install a firewall. A strong firewall can act as a deterrent to intruders, forcing them to look for other ways into the system. In its original incarnation, firewalls were computers that protected the local networks and dial-in lines by controlling information that was let in or out (Benson, 1998a). Today, one can obtain a "personal firewall" which runs on an individual client machine and offers a similar level of protection.

For example, Zone Alarm 2.0 (http://www.zonelabs.com/) is freeware that will install a "personal firewall" on each machine in the network. Alternatively, a number of vendors offer network firewalls that operate off a dedicated machine.

If a user has legitimate business on your server, the most common compromise of data is most likely accomplished with good intentions—the client introduces a computer virus. A virus is actually a program that can destroy, delete or "lock up" information and applications on a system. If data is not damaged, the virus can still be troublesome in that it takes up valuable disk space and memory. Viruses are often attached to some sort of host program, where the execution of the program causes the execution of the virus. These programs commonly take the form of Trojan Horse viruses. The Trojan Horse virus performs its action covertly and is delivered via a host program or "dropper" (McClure, Scambray, & Kurtz, 1999).

These viruses typically enter the computer system in one of three ways: by disk, downloads, or attachments. Floppy disks used on other systems can be used to unwittingly "transmit" the virus when opened on another system (Campbell, Robertson, & Harley, 2000). Downloading information from any online service can introduce virus programs. Lastly, e-mail attachments carrying a virus, if execution is tied directly to the opening of attachments by the e-mail system, carry the potential to damage systems. Often reports of these are exaggerated and many of them are hoaxes, but the possibility does exist. There are several web sites that list the names of popular virus warnings that are typically sent via e-mail. These web sites differentiate between warnings that are hoaxes and those that are actual threats (Thornloe, 2000).

Anti-virus software is the most common protection from this type of threat. When looking to choose an effective anti-virus program, there are some factors that should be taken into account in order to insure the best fit with the intended system. First, the type of system can make a difference. Second, is the system networked and if so, should the entire network be protected? Finally, check the types of virus detection and prevention offered by the software. One option that a good virus protection program should offer is the ability to receive virus protection updates from the company. This updated information should help protect systems from newly developed viruses. Two types of scanning practices are used in virus detection. Signature-based scanning should be used to detect the virus before it is brought into the system and before the opportunity arises for it to activate. One way this is accomplished is through heuristics-based scanning, which is a program that checks for codes commonly used to create viruses. Another method is using memory-resident monitoring to check the memory for an existing virus. The software should also regularly check the integrity of program files to determine whether changes have occurred. Companies such as McAfee or Symantec provide various types of anti-virus software depending on the needs of the system. There are also free anti-virus software or "freeware" that can be downloaded from the Internet.

One frequently employed security measure, used when sensitive information is transmitted from one source to another, is encryption. Encryption is the transformation of data into a form that is nearly impossible to read without the use of a key (Schneier, 1996). This provides a safe way to send sensitive information, like test banks or subject information, to other locations via the web. Information is first transferred into an encrypted, or unreadable, form and sent to a certain destination. Once it arrives, an authorized party uses a key to decrypt, or decode, the information. In a public and private key system, the public key is shared among authorized users and is used for encryption only. Once the information is received, it can only be decoded by the recipient's own private key. The private key is accessible only by individual recipients. Secret key systems are also employed, in which both sender and recipient encode and decode information with the same key. However, it can be difficult for both parties to agree on a particular key without the fear of someone else discovering this information. These keys generally have life cycles that eventually cause them to expire, which insure that new keys are constantly being developed and used (Schneier, 1996). This is very important considering the common uses for encryption. Sensitive data can be transmitted and shared with little fear of being lost or stolen, if the encryption software is effective and current and if the program has been implemented properly. When data are successfully intercepted and decrypted, it is rarely because the actual code has been broken. Often it is easier for intruders to look for holes in the implementation. Lapses in security are much easier to exploit than the complex methods employed by encryption programs.

What Now?

Perhaps your web site has been compromised, but you have finally figured out the problem, and have employed security experts to deter further incursions. Are you out of luck? Depending on the length and extent of the data compromise or loss, you may still be able to reconstruct some of your data, IF you have backed up on a regular basis. Contingent on the malicious nature of your intruders, you may still be able to retrieve data from your original server or hard disks. For example, some programs that "erase" data only eliminate the file name from the file allocation table; the actual data may still reside on the hard disk until overwritten by some other file. File management programs like Norton Utilities may be able to unerase files that have been "eliminated".

It is quite likely that the future portends well for improving the security of web-based data collection procedures. Computer security programs have become more sophisticated in protecting computers connected to the Internet. Moreover, increased sensitivity on the part of consumers has heightened awareness of potential problems in this arena. However, as data collection mechanisms become more complex, the complexity will breed opportunities for hackers looking to disrupt or compromise the integrity of information that is collected through the World Wide Web.

The moral of this article is that one can never be too careful when it comes to evaluating both the motives of people and the capabilities of technology—most of us tend to underestimate the good intentions of those around us and overestimate the wizardry of machines. By taking a systematic approach to evaluating the security of your test site, you can avoid the embarrassing prospect of asking, "Where did all the data go?"

Appendix A: Selected Places to Visit About Security

Hacking Exposed www.hackingexposed.com

RSA Security Homepage www.rsa.com

Computer Security Institute www.gocsi.com

Computer and Network Security Index

www.vtcif.telstra.com.au/info/security.html

Virus Bulletin www.virusbtn.com

Computer Security Information www.alw.nih.gov/Security/

UN on Computer-related Crime

www.ifs.univie.ac.at/~pr2gq1/rev4344.html

COAST Security Archive Group

www.cerias.purdue.edu/coast/archive/

Network Security Library www.secinf.net

References

Benson, A. C. (1998a). Securing PCs and Data in Libraries and Schools: A Handbook with Menuing, Anti-Virus, and Other Protective Software. New York, Neal-Schuman Publishers, Inc.

Benson, A. C. (1998b). "Building a Secure Library System." Computers-in-Libraries, 18(3), 24-26, 28-29.

Brandt, S.,(1998). "Insecurity on the Net." Computers-in-Libraries, 18(3), 34-37.

Bridis, T. (February, 2000). Hacker victims or accomplices? Associated Press Technology.

Campbell, R., Robertson, P. & Harley, D. (2000). Computer and Network Security Reference Index. (website) Available: www.vtcif.telstra.com.au/info/security.html.

McClure, S., Scambray, J., & Kurtz, G. (1999). Hacking Exposed. Berkeley, Osborne/McGraw-Hill.

Schneier, B. (1996). Why Cryptography is Harder Than it Looks. (website) Available: www.insecure.org/stf/whycrypto.html.

Shermis, M. D., Mzumara, H.R., Lillig, C., & Brown, M. (1997). Computerized adaptive testing through the World Wide Web. Presentation given at the annual meetings of the American Psychological Association, Chicago, IL.

Thornloe, F. (2000). Virus Bulletin. (website) Available: www.virusbtn.com.

Author Notes

Correspondence concerning this paper should be addressed to Mark D. Shermis, IUPUI Testing Center, 620 Union Drive, Indianapolis, IN 46202-5168. Electronic mail may be sent via Internet to MShermis@IUPUI.Edu.

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

REPRODUCTION RELEASE

(Specific Document)

I. DOCUMENT IDENTIFICATION:

Title: Security for web-based Tests

Author(s): Mark D. Shermis & Jason Averitt

Corporate Source: Paper presented at the annual meetings of the American Educational Research Association, Seattle, WA.

Publication Date: April, 2001

II. REPRODUCTION RELEASE:

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, *Resources in Education* (RIE), are usually made available to users in microfiche, reproduced paper copy, and electronic media, and sold through the ERIC Document Reproduction Service (EDRS). Credit is given to the source of each document, and, if reproduction release is granted, one of the following notices is affixed to the document.

If permission is granted to reproduce and disseminate the identified document, please CHECK ONE of the following three options and sign at the bottom of the page.

The sample sticker shown below will be affixed to all Level 1 documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

Level 1

☒

Check here for Level 1 release, permitting reproduction and dissemination in microfiche or other ERIC archival media (e.g., electronic) *and* paper copy.

The sample sticker shown below will be affixed to all Level 2A documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE, AND IN ELECTRONIC MEDIA FOR ERIC COLLECTION SUBSCRIBERS ONLY, HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2A

Level 2A

□

Check here for Level 2A release, permitting reproduction and dissemination in microfiche and in electronic media for ERIC archival collection subscribers only

The sample sticker shown below will be affixed to all Level 2B documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2B

Level 2B

□

Check here for Level 2B release, permitting reproduction and dissemination in microfiche only

Documents will be processed as indicated provided reproduction quality permits.
If permission to reproduce is granted, but no box is checked, documents will be processed at Level 1.

I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as indicated above. Reproduction from the ERIC microfiche or electronic media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries.

Sign here, → please

Signature: Mark D. Shermis

Printed Name/Position/Title: Mark D. Shermis, Professor/Assoc. Dean

Organization/Address: Florida International University
ZEB 310
Miami, FL 33199

Telephone: 305-348-2092

FAX: 305-348-2081

E-Mail Address: mshermis@fiu.edu

Date: 9/12/01

(over)

III. DOCUMENT AVAILABILITY INFORMATION (FROM NON-ERIC SOURCE):

If permission to reproduce is not granted to ERIC, *or*, if you wish ERIC to cite the availability of the document from another source, please provide the following information regarding the availability of the document. (ERIC will not announce a document unless it is publicly available, and a dependable source can be specified. Contributors should also be aware that ERIC selection criteria are significantly more stringent for documents that cannot be made available through EDRS.)

Publisher/Distributor:

Address:

Price:

IV. REFERRAL OF ERIC TO COPYRIGHT/REPRODUCTION RIGHTS HOLDER:

If the right to grant this reproduction release is held by someone other than the addressee, please provide the appropriate name and address:

Name:

Address:

V. WHERE TO SEND THIS FORM:

Send this form to the following ERIC Clearinghouse:

University of Maryland
ERIC Clearinghouse on Assessment and Evaluation
1129 Shriver Laboratory
College Park, MD 20742
Attn: Acquisitions

However, if solicited by the ERIC Facility, or if making an unsolicited contribution to ERIC, return this form (and the document being contributed) to:

ERIC Processing and Reference Facility
1100 West Street, 2nd Floor
Laurel, Maryland 20707-3598

Telephone: 301-497-4080
Toll Free: 800-799-3742
FAX: 301-953-0263
e-mail: ericfac@inet.ed.gov
WWW: http://ericfac.piccard.csc.com