Global Information Assurance Certification Paper

Laurie Hoyler Schumann
Version 1.4

Event Auditing and the use of the Transaction Life Cycle

A transaction life cycle approach for event auditing provides an enriched overview of security policies and the understanding of them. Often overlapping, specific issues or concerns can be blurred with the dizzying array of logs generated and other alerts raised. Determining a user's understanding of security policies or determining their appropriate use of the system is often a neglected task, by disassembling the audit or drilling down on one level of the transactions life cycle, areas of strength and weakness can be readily identified. By using the differing levels for classification of reports, future audits can be generated demonstrating the effectiveness of recovery and education efforts or the overall security policy.

While it is the organization's security policy that will set the parameters for maintaining the state of "acceptable risk," it is through audit that the effectiveness of this policy will be measured. Audit will also help develop an intuitive security policy where one does not yet exist. However, audits of information technologies are often thought of as yearly events for organizations done to provide risk analysis and quantify the results for accounting purposes. This type of audit is required for certain situations, such as government certification and accreditation or regulatory mandates by VISA for example. Not all organizations need to meet criteria of standards such as government certification and accreditation, and therefore SOPs may not be established. It is hoped that this very basic information can be utilized by a wide range of businesses including the very smallest of firms, many of which "depend on computerized data...for the entire business," according to the Small Business Administration and are extremely vulnerable, "due to it's concentrated form." (Crime 7) A method needs to be developed that insures that the security policies are enforced and those users of the information systems accept and understand their role and responsibility in it. These audits, referred to as event auditing, while not usually established as upper management concern until a system becomes compromised, are essential to the "everyday, year-in-year-out" assurance of the continued reliability and availability of the IT systems.

We begin by making a few assumptions: Information security has been established as a management priority. The appropriate hardware, including firewalls, have been installed with physical and environmental issues resolved. An intuitive information security policy has been implemented. Standard operating procedures (SOPs) have been developed to maintain the various components of the system and its' software in a hardened state. It is at this point that many organizations underestimate or fail to recognize the value of vigilance for identifying weakness or vulnerbilities to its networks. Quite simply put, they fail to audit for compliance. Although the news media focuses on

external threats, (i.e. the Internet with its viruses, Trojans and worms), it is often activities within the organization and the organization's posture on the use of their own systems that leave them vulnerable.

Event Auditing

Event auditing falls into two classes: informal and formal. What differentiates an informal audit from a formal audit is that of an applied standard to validate or invalidate a procedure. Many known standards adapt well to manual checklists that can be applied to actual procedure. The information security policy with support of an acceptable use policy offers just such an opportunity for a formal audit. What is better, there are tools available to automate the task. If an organization's security policy, assuming one exists, does not address the frequency of this type of audit, then a doctrine of "changes" should be adopted—any change equates a formal audit. For simplification, a change can be but are not limited to any of the following: operating system patch, application upgrades, new application implementation, new use of existing technologies, new hire or fire, new hardware installation, reorganization, change of accounting month, change of user's network use habits, hardware failure. It should also be noted that automated tools used for auditing provide a wealth of information that can become overwhelming if not dealt with on a routine basis. Informal audits, while not defined by a set procedure or rules, is effective in establishing the need to develop a standard or ascertain a user's understanding of responsibility. In either case, auditing should at the very least address the following areas:

Know Thy System.

Before any system can be audited, it has to be identified. First and foremost, it must be identified as falling under the designated auditor's authority. To scan, collect data (including logs) or create scripts on systems not under one's authority is in many instances career ending if not illegal. While it is true that an organization's information security is only as good as the weakest system on the network, to forge into another's domain without explicit permission is not the example the security conscious administrator wants to set. This requires understanding how the networks were designed and implemented especially if and how they interact with each other. Once the topography has been mapped, attention must be turned to the details of the system to be audited. When documenting the configuration of the system make sure to include the following:

1. Architecture: the operating system and version with any Service Packs or Hot Fixes
2. Hardware
    a. CPU
    b. Memory
    c. Disks

        1. Hard Drives and Partitions
        2. Removable Media: floppy drives, CD-ROMs, etc…
    d. Peripherals: keyboard, serial devices, smart card readers
3. Machine Name and IP address
4. List of running processes
5. List of well known services not running (by experience)
6. List of remote procedure call (RPC) services
7. System interfaces (i.e. network interfaces)
8. Data and Information
9. System's value or importance to the organization
10. Level of protection required to maintain system and data (integrity, confidentiality, and availability)
11. Persons supporting and using the system
    a. Technical Support
    b. Application Users
    c. Non-blocked accounts

Any audit will utilize this information, whether in parts or sum total. Therefore, it is imperative that it is kept current at all times. The Caveat: It is difficult to detect network misuse or compromise when the systems are known to the System Administrator, failure to keep current on the systems increases the risks of compromise. Often times referred to as baseline, an event audit of this information as changes occur provides for an accounting of actions and provides for summary evidence without having to publish the details of a system's configuration.

Authentication, Proof of Identity

Identification and authentication of a user is a very important test of the security of a network and passwords in conjunction with logins are oftentimes the means to validate or invalidate network access. With this in mind, regular, consistent audits need to be performed to ensure authentication has not and cannot be compromised easily.

One of the hardest concepts for average users to comprehend is that of passwords. It is not an understatement to say that password education is a continual process and should be addressed through formal and informal means. Password policies attempt to address several misconceptions and lazy tendencies. To mention a few, a password is not a personal identification number (PIN), not a birthday or anniversary, and it is not a name or chorus to a song. In fact, it's not supposed to be memorable or obvious to anyone except the creator. Second, to debunk the idea that a fellow employee who someone works with for years is not capable of doing anything malicious or damaging. Third, to negate the threat of any non-employee (visitors, tradesmen, cleaning crews) of compromising the system. Informal review of password policies should be conducted quite regularly. Informal audits can be conducted in a

variety of ways. One of the most effective is perhaps the simplest--simply looking at and around workstations walking through the office or complex. Once the post-its begin to reappear, it becomes obvious that users have become complacent and need to be reminded of their importance in the "fight against crime." Although this is termed an informal audit, you must still define and develop this audit to acceptable criterion so that "Recovery" (to be discussed later) can be documented. Formal review would be difficult if it were not for password-cracking programs such as Crack, LC3, or John the Ripper. These tools when allowed provide versatile functionality as well as providing evidence to hold the users accountable for not using a strong password or for using the same password to access several services.

Formal Auditing of Password Policy should also include verifying the network's configuration of password controls any time a change is made (i.e. service packs or patches installed). Controls to verify would be: complexity; aging, such as minimum and maximum; history, how to verify a user doesn't reuse passwords; storage of passwords with one-way encryption (hashes); where and how the password files are stored; account lockout policy for attempts (threshold); duration of account lockout; and reset of account after lockout, testing against dictionary databases.

While this is great for accounting of proper system setup that essentially leads users down the appropriate avenue and provides some protection from brute force attacks, it does not provide assurance of effective authentication. By examining the logs, one should audit for failed logons. Failed logons may indicate that the system authentication process is being tested to eventually lead to compromise. Brute Force Attack is defined by literally trying to guess the password of the targeted user, hence the failed logon event. As this is not the only means to compromise a system, you should also audit successful logons then compare them to known user habits. For example, *model* logs into the system at and around 8:30 AM with a scattered mentions throughout the day but never after 4:30 PM and never on weekends. To find a successful logon entry for *model* on Sunday at 2:30 AM would be alarming. Although this does not provide evidence of user's compliance to the security policy, it is a great introduction to another common problem.

Training an employee not to leave their workstation with open sessions is a daunting task. Here again, walking through a facility around lunchtime can provide clues to the level of compliance being met. Careful review of the logs can provide snapshots to user habits. Although it would be difficult to use this information as evidence to hold a user accountable, it will indicate if this person should be reminded of the security policy or if their accounts need further restrictions. This problem should also be addressed through security settings, such as restricting the length a time a person can be logged on without having to be re-authenticated or through the use of password protected screensavers.

The procedure for changing a password should be very familiar to all users and therefore it should be well tested. Because writing passwords down is against security policy, passwords will be forgotten. The steps to validating of the user who is requesting the change needs to be tested, and the change log verified. If exceptions are to be made to the policy, burden is placed to follow up and monitor the user and these events have to be part of the audit process. Also, it is imperative that users be familiar with the procedures that will be implemented by system administration when passwords on a system need to be changed quickly. Hence, there is another informal audit that is critical to evaluating a user's understanding of their part in keeping their password private. It is easy to assume an average user knows that any request for a user's password or asking them to change it to a provided value is a bad security practice if not a specific cause for alarm. The easiest example to provide a user is that of America Online. AOL realized the need to educate their users by instituting banner warning messages at popular points of compromise, such as their AIM program, stating in effect that no one would ask for your password and if someone does they should be reported. As this is a very popular ISP for home users, most have seen this warning. Does it translate well to users in the work place? Without developing a scheme to pose the question, it will go unanswered. Surprising results, and disappointing given the positive number of responses, were garnered by developing an Email that is in direct contradiction to the Information Security Policy and dissimilar to the procedure to follow in the event passwords need to be changed. While no information was actually exchanged, it should have generated reports of suspicious activity, not requests for password changes.

Authentication concerns do not start or end with passwords or unattended workstations, although not directly related to user compliance it would be improper not to provide honorable mention of secure remote access/authorization services such as SSH, RADIUS and Kerberos for addressing authentication concerns. Once the user is authenticated though, one's attention must turn to account related events such as object access, policy changes, privilege uses and system events.

Access Control

Assigning of user rights and privileges are often defined by job descriptions with the idea that "less is more." Assigning of users to descriptive groups does help provide guidance on what known rights and privileges should be assigned to define access control. Just as it is inappropriate to allow a default software installation to determine user access (i.e. Guest user, Anonymous User) and privileges, it is improper to assume that those rights cannot be tampered with or improperly defined to begin with. Therefore, one must be vigilant in comparing Users and Groups to the baseline. Following is a breakdown of events to monitor for:

1. Routing
    a. Service-Filtering ACLs
        Such as those used by TCP Wrappers
    b. ARP, DNS
2. Privileges
3. Root and Super User commands
4. Trusted Domains
5. Running Services
    a. Scanning for known Vulnerabilities
    b. Printing, installation of Print Drivers
    c. Cron Jobs or Task Schedulers
6. File System Integrity
7. Registry entries
8. Loaded drivers
9. File Access
10. Logon Access (network, local, remote, etc.)
11. System events such as shutdown or reboot

Use of vulnerability scanners should also be instituted periodically. Network Vulnerability Scanners provide a glimpse of known vulnerabilities from the outside looking in perspective. Host Vulnerability Scanners operate at the system level and provide polling of security policy related events. Other Access issues are as basic as the workstations themselves.

Users generally do not understand the controls afforded by the Information Security Policy, as such, verifying that unneeded removable media devices such as floppy drives and CD-ROMs are disabled is a safety practice all to itself. For example, most general users on the Internet do not understand how to read a site's certificate to determine if it can be considered a trusted site. Therefore, any software brought in may be contaminated. It would also be unadvisable to allow the introduction of untested software that may conflict with current applications. This demonstrates the need to perform an audit to ensure that users haven't bypassed the safety mechanisms. When disabling floppy drives and CD-ROMs it becomes obvious that there needs to be controls in place to protect the computer's system BIOS from alteration of desired set up. This is usually accomplished through password protection of the BIOS. Traditionally though, one would simply have to reset the CMOS to restore the BIOS to factory defaults to remove the password protection. The occurrence of this event would not necessarily be obvious to anyone except the regular user of the workstation hearing a floppy seek at boot, informal auditing for understanding of this system state should be done. The other desire would be to verify that if these devices were enabled for a specific exception, that they were disabled again.

Connecting a workstation's modem to a phone line presents another security risk that might be consideration at the Access level. That is, a phone line is not routed through a firewall or site router and thus it opens a very viable venue for

attacks. One of the many reasons a user may connect a phone line to their workstation without submitting a formal request can be as simple as the perimeter firewall blocking of web sites they wish to access. It may seem harmless to them, but the firewall is blocking those sites for a reason. The use of Wardialers on internal phone lines should be used to scan for these devices. A separate but not unrelated concern arises with using the modems for faxing from the desktop or use of modem for uploads. If this is allowable, it should be verifiable that only outbound faxes are allowed locally. Incoming faxes should continue to be directed to dedicated fax machines.

Any deviation from the expected is cause for great concern, obviously automated logs from all services and applications must be compiled and checked, not just the server operating system. But the logs themselves can become suspect; therefore, they must withstand a certain level of validation and protection.

Logging

Logs are the wealth of information of what was done or being done, when and how, and it has to be parsed into usable information. Confirming what logs are generated and what information is being logged is essential in providing a "big picture" of system activity. This includes the personal firewall logs installed on the individual workstations. Capacities should be monitored and the logs themselves need to be centralized away from a system that could be targeted. Alert mechanisms need to be tested. Procedures for analyzing and archiving logging results have to be audited. Log maintenance, such as clearing a log so that new information isn't just appended to the end of the old, itself needs to be logged to assure the audit trail.

Although it is common sense that one should audit the logs for any deviation of "normal", it is just as important to audit the logs for expected events. Naturally the first thought is that it is essential to know the expected to identify the unexpected. As true as this is, being able to show consistency in expected values between audit periods provides for verification of how effective the Information Security Policy is at achieving the "acceptable risk" level of system confidentiality, integrity and availability. The problem arises however that logs can be compromised, so to further support the audit of the log, tools become essential in substantiating those findings.

Intrusion Detection

There is a myriad of tools available to aid in intrusion detection and plenty of lists with descriptions of each of the tools on the internet to help guide the decision of which tool works best for a system or security concern. Use these sites for information purposes. But always verify that a source is trusted before downloading any script.

Federal Computer Incident Response Center (http://www.fedcirc.gov/tools.html)
Unix Host and Network Security Tools (http://csrc.nist.gov/tools/tools.htm)
Unix Network Security Tools (http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html)
Tools (http://www.hackingexposed.com/tools/tools.html)
IDS Overview (http://www.networkintrusion.co.uk/ids.htm)

However, there is not an all powerful, all encompassing tool, so one must be willing to learn and use these tools in combination to attain the needed results. Because internal threats circumvent organization's perimeter firewalls, many of these same tools will be used to baseline the system at the access level.

Using a logging utility to enhance system log abilities to detect misuse maybe desirable. For example, LogSentry (http://www.psionic.com/products/logsentry.html) monitors for security violations and will periodically email them to you. Logsurfer (http://www.cert.dfn.de/eng/logsurf/) monitors logs in real-time.

Intrusion Detection involves recognizing behaviors as well as preventing known vulnerabilities to remain unapprised. Of the ways to check for system misuse is that of comparing known attack signatures, looking for anomalies within the protocol, or packet sniffing. This is a job usually provided by Network Intrusion Detection Systems (NIDS) such as Snort (www.snort.org).

Of course NIDS does not focus on host services nor does it scale well to switched networks, with this in mind Host Based Intrusion Detection Systems (HBIDS) should be implemented. Uses provided by HBIDS are logging of packets and checking them against an ACL, port scan detection (including stealth scan), create and maintain cryptographic hashes of file and drops modified files. An example would be Tripwire (ftp://coast.cs.purdue.edu/pub/tools/unix/).

When using such a powerful suite of tools, it would be hard to imagine a system being compromised. Due caution should be exercised though, any tool that is utilized needs to be tested and protected. Methods of storing and configuring the tools should be documented and audited routinely. Results should be examined to ensure accurate recording of desired events. But one cannot end an audit for malicious activity at this level, it would leave you with little assurance of the continued availability and reliability of your systems.

Availability/Reliability

The use of quotas allows for assurance of availability. When a system is setup, partitioning with the setup of quotas in mind lend to the availability of the system. By the same token, establishing quotas for use by an application, service or user can be used to test for malicious activity or accidental overwrites. This is especially important in Unix with regards to the temp directories or sharing of User IDs. It should also be mentioned that log files and backup

system sizes should be logged in that their usage can be monitored and therefore leave ample room for archiving and or better planning (i.e. tape rotation).

Backup and Redundancy provides for special security concerns on several levels. Anyone who has had a backup mechanism fail, only to be discovered when a restore was needed knows that sick, sick feeling. Yes, it is easy to point the finger because policy was not followed or the procedures were not well understood, but the truth be known, audit of each component would have provided evidence of needed change, whether it be procedural, mechanical, or reassigning of duties due work load.

An archived backup to tape media or other removable media presents the hazard of storage. In the introduction of this paper, we made the assumption that all physical and environmental concerns were provided for. But the human factor has not been addressed. Logs of activities regarding tapes and tape drives (i.e. cleaning) need to maintained and audited for events. Such as, if using Differential Backups with a weekly Full Backup, is the filling up with data on a tape monitored and the tape then rotated out and properly stored. When sending tapes off-site for storage, are events logged such as identification of tape, handler, date and time? When stored on-site, are they sufficiently labeled so that the data does not get overwritten prematurely? Are the mechanisms to actually test the integrity of the media itself being implemented? An analogy often used is that of handling tapes as one would a huge financial transaction such as the transportation of the organization's assets. As alluded to earlier, small businesses very well may be transporting their assets in the form of one single tape (financial records such as payroll, general ledgers and inventory, customer databases, business plans including detailed production commitments). As this demonstrates the particular value of this audit for small businesses, it should be noted that while they may not need to meet the criteria of government accreditation they will have to meet the burden of adequate backup controls for business insurance purposes. The guiding principle here is that loss or theft of a backup tape, for large as well as small organizations, can have extremely devastating consequences.

Redundancy, like tape media, has its mechanisms that need to be verified. Improper configuration can translate into no method of restore. Audit of the policy, testing of the hardware, ensuring strict access rights as well as the use of encryption is essential.

Although touched upon with the disabling of floppy drives and CD-ROMs, it would be inappropriate not touch upon the methods used for system repair. This includes addressing how the Emergency Repair Disks (ERD) or Boot Disks handled and stored. Without proper restore controls in place, recovery becomes cumbersome and time consuming and could translate into down time.

Recovery

Any good Information Security Policy should address the issue of recovery. Usually when we think of recovery, it is in terms of incident handling of extreme natures. As such Incident Handling procedures should be tested before a devastating event occurs. It makes since to perform a dry run with as many as possible responsible parties involved so the effectiveness of the response can be measured. Do they have a plan? Do they know whom to contact? Do they have the necessary tools to do the job? Do they know when to escalate the alarm? If a more knowledgeable contact is needed, is this information readily available? Detailed logs of all actions taken must be kept, including those related to restoration of the system and actions taken to address the security breech. Follow-up audit of each step of these actions provides clear-cut analysis of the actions taken and the success of the policy. With this said, it is the aforementioned audits of users and user understandings themselves that will generate incidents and as such, upon completion of each audit, its recovery should also be documented.

A summary of recovery results may best be categorized by using the above mentioned processes of a Transaction Life Cycle. An extremely simple example: Tom reports he cannot find a report he knows he saved to his user directory. Upon inspection, this file is found to be located in Jane's directory with her ownership rights. Examination of logon activity for the time period indicated Jane never logged off the workstation and Tom never logged on. This is an authentication failure that resulted from breech of security policy. Because Event Auditing is often thought of in terms of being based solely as reading logs and generating reports based on their contents. Also, since subjects of event audits tend to focused and specific, based on the training the auditor, it would be possible to overlook cause/effect relationships. By classification of events it would be suitable to file the results for this report under authentication to be used for future audits of the effectiveness of recovery measures. Such as, are current user education efforts working? Furthermore, it would be true to say that management does not necessarily understand the full process of computing. Finding a man-in-the-middle attack will not necessarily hold their interests if they do not understand the nuances. Thus, the Transaction Life Cycle lends its own layers, enhancing event auditing and understanding for subject matter.

Works Cited

United States. Small Business Administration. Curtailing Crime, Inside and Out.
http://www.sba.gov/library/pubs/cp-2.pdf

References

Coggins, Deborah. "Computer Incident, Intrusion, Emergency Response Audit Program." May 2001. http://www.auditnet.org/docs/CIRT_Audit_Program.doc

Hatch, Brian, James Lee, George Kurtz. Hacking Linux Exposed: Linux Security Secrets & Solutions. Berkeley: Osborne/McGraw-Hill, 2001.

IT Security Cookbook – Securing Unix #2. 30 Mar. 2001 http://www.boran.com/security/unix2.html.

McCollum, Tim. "Managing Security Policies." ITAUDIT.org. Vol. #5. 15 Aug. 2002. http://www.theiia.org/itaudit/index.crf?fuseaction+print&fid=477

"RFC 1244 – Types of Procedures." http://www.net.ohio-state/rfc1244/types.html.

Shawgo, Jeff, ed. Windows 2000 Professional Operating System Benchmark Consensus Baseline Security Settings. Ver. 1.0. The Center for Internet Security. 17 July 2002. http://www.cisecurity.org

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology Special Publication 800-30. Washington: GPO, 2001. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf