Global Information Assurance Certification Paper

A Forensic Argument for Network Time Synchronization
Belinda Brockman
Level One_Security Essentials

It is obvious to most system administrators that workstation, server and routers logs are valuable sources of information and evidence. These logs are used not only to monitor the performance of the computers, systems, and networks; but also to analyze the patterns of events and incidents within a computer and its network. As Girardin notes: "One of the primary sources of information that enable support for system administration is the logging facilities provided by key system components. Such facilities are often used to track real-time events triggered by system, user, and network activity. Continuously monitoring this activity is of tremendous importance to organizations which rely on high security [Geer, et al., 1997] and optimal resources availability. Logs provide support for proactive system maintenance, anomaly and intrusion detection, failure analysis, and usage assessment."(1)

In both the NT and Unix auditing courses taken as part of Level One GIAC training, commands (such as syslog or dumpel), scripts, and reasons for assembling, and reviewing computer logs have been presented. These actions are urged to become routine security practices, because as Action 1.8.3 of *Computer Security Incident Handling: Step by Step (CSIH)* (2) notes " the indicators of many never detected incidents are buried in log files. It is not enough to collect system logs, it is important to also read them." In addition, the use and importance of logs as evidence is acknowledged in *Action 2.3.2 Identify Evidence CSIH*, and in *Actions 3.5.1 and 3.5.2* CSIH to acquire router and system logs and review the logs form neighboring systems.

Similarly, the importance of logs in security is emphasized in information security auditing when auditors are advised to determine the policies related to the configuration of system audit log facilities; to evaluate if appropriate events are being logged, and appropriately secured, backed-up and archived. (3)

There is, however, a dark side to using computer logs. They, like any other piece of evidence, must be admissible to be used in court. * In computer forensics and incident handling discussions, the importance of preserving the chain of custody, and of being able to demonstrate the authenticity, reliability, and relevance of evidence is stressed. These actions are necessary to meet the required tests of authentication, and reliability of evidence. What is rarely pointed out, however, is that the computer logs from which we draw much of our analysis are by definition hearsay. As Tipton and Krause note: "A legal factor of computer generated evidence is that it is considered hearsay. Hearsay is second hand evidence; evidence which is not gathered from the personal knowledge of the witness but from another source. Its value depends upon the veracity and competence of the source."(4)

As the DOJ's pamphlet on the *Admissibility Of Electronically Filed Federal Records As Evidence(5)* states: "It should be noted that the rules of evidence are no different for electronically filed records than for paper records. However, because electronic files are particularly susceptible to purposeful or accidental alteration, or incorrect processing, laying a foundation for their admission must be done with particular care. Proper control over creation and maintenance of these files can be crucial in overcoming inevitable

objections that will be raised in the courtroom."(5)

Common exceptions to the hearsay rule involving business (and official) records, the so called business exemption (Federal Rules of Evidence 803(6)), allow a court to admit reports or other business documents introduced by a competent witness which are made:

- at or near the time,
- by or \from information transmitted by a person with knowledge,
- if it was kept in the course of regularly conducted business activity,
- and it was a regular practice of that business activity to make the report or document because it was relied upon by that activity. **

These requirements lay a tremendous burden on the system administrator. To be admissible as evidence, his logs must be demonstrated to be not only relevant, and reliable, but also to be a regular part of business. For as Tipton notes: " If the audit trails are not used or reviewed (at least the exceptions – i.e., failed log-on attempts) in the regular course of business, then they may not meet the criteria for admissibility." (4) Fortunately, the logs no longer have to be introduced by expert witnesses but rather can be introduced by a competent system administrator.

On the surface, these facts present an obvious argument for requiring review and reporting on audit trails from servers, etc.; advise which has been stressed over and over. But the requirements to validate logs as business records also present a more subtle argument for the imposition of a uniform time source within an enterprise. To attempt to consolidate and trace the actions of an intruder through logs that are not based on a such a standard time source, is difficult at best. Events that occur subsequent to one another are recorded as simultaneous. Transactional or time line analysis becomes complicated and requires detailed explanations to explain why variation in time exists.

The question then becomes why is then need for a uniform time source not mentioned in the normal literature of on computer forensic examination or standard audits. In the standard forensic analysis of a computer for an incident, the dates and times of events can be taken relative to the time of that computer. Experts give such advice as: "The contents of the CMOS, as well as the internal clock are checked and the correctness of the date and time is noted. The time and date of the internal clock is frequently very important in establishing file creation or modification dates and times**.** "(6) Specialized software such as GetTime has been developed to allow the examiner to document the system date and system time settings of the subject computer. For as the software developer notes, "File dates and times associated with allocated files and previously deleted files can be important in cases involving computer evidence. The reliability of the file dates and times are directly tied to the accuracy of the system settings for date and time on the subject computer. Therefore, it is important to document the accuracy of the system clock as soon as possible. Low battery power or day light savings time changes are likely sources of system clock inaccuracies. This program aids in the documentation of the system clock settings for time and date. When the dates and times that files were created, modified or last accessed, this information is relevant." (7)

Such a luxury is often not available in analyzing or tracing events through a network due to the number and variability of the computers, routers and operating systems involved. Yet the issue of uniform time is rarely considered in some organizations. There are numerous reasons why a large institution may function practically without a uniform time source. For organizations running a single network operating system such as Novell with NDS, time synchronization disciplines are necessary to keep the NDS traffic in order. But in multi-platform institutions, each network, in reality, has its own way of synchronizing time and keeping track of its transactions. Within a system, the variations in time among the machines are often smaller than the variations needed to be tracked. It is only when the analyst attempts to track actions across multiple networks and computer systems that the difference in time becomes a hindrance. Without a uniform time source, the transactions of each device have to be translated to a some uniform time before analysis can begin.*** While such analysis is possible, the need to demonstrate such analysis would be *prima facie* evidence that the logs were not reviewed in the regular course of business thereby obviating the point of performing it.

NOTES:

* For reasons why administrators should be concerned with court presentation of records, individuals should note that: “Because of their ubiquitous nature documents stored in electronic form... should be specifically targeted by counsel in developing their discovery plans. Failing to do so may not only prejudice their case, but may also constitute malpractice." Michael R. Overly, California Continuing Education of the Bar (1998 3d Ed), Civil Discovery Practice 3rd Ed., Vol. 2, §8.24, pg. 711, http://californiadiscovery.findlaw.com/El%20Disco.htm and read the articles on “Effective Discovery of Electronic Evidence” and “Electronic Discovery of Computer Based Evidence” at Http://www.forensics.com/resources/discov.htm.

**For a fairly complete discussion of the electronic documents as evidence, individuals are encouraged to see *Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment*, published by The State Archives and Records Administration, New York State, http://www.archiveindex.com/laws/law-ny.htm.(1994)

*** Synchronizing time within a network is a full subject in its own. Individuals interested in the topic are encouraged to visit Http://www.eecis.udel.edu/~mills/bib.htm for a bibliography of articles on Computer Network Time Synchronization or Http://www.eecis.udel.edu/~ntp/ntp_spool/html/exec.htm for an Executive Summary discussing the issues, techniques, and security risks posed. In addition, the need for a uniform rather that individual time sources for each server becomes more obvious when one realizes that there are differences in UCT and GMT due to the introduction of leap seconds in the UCT clocks.

References:

(1) Luc Girardin and Dominique Brodbeck *A Visual Approach for Monitoring Logs* - UBS, Ubilab; URL: http://www.usenix.org/publications/library/proceedings/lisa98/full_papers/girardin/girardin_html/girardin.html (1998)

(2)Northcutt, Stephen; Computer Security Incident Handling: Step by Step, version 1.5 The Sans Institute, 1998.

(3) Heckendorn, Sherri; "*Auditing NT Security*", pgs 3&4, The Sans Institute URL: http://www.sans.org/y2k/practical/Sherri_Heckendorn.doc (Feb. 2000) and Turcato, Lance M.; "*Logical Security: A Generic Audit Work Program, Objective G*", San Fransisco Chapter #15, Information Systems Audit and Control Association, URL: http://www.sfisaca.org/resources/genaudipgm.htm

(4) Tipton, Harold F. and Krause, Micki; Information Security Management: Handbook, 4th edition; Welch, Thomas "*Computer Crime Investigation and Computer Forensics*, pgs 609-610; 2000, CRC Press LLC, Boca Rotan, Fl.

(5) Various, *"Admissibility Of Electronically Filed Federal Records As Evidence*," U.S. Dept of Justice, Justice Management Division, Systems Policy Staff, Oct. 1990, URL: http://www.lectlaw.com/files/crf03.htm

(6) Unknown," *Hard Disk Examination";* The International Association of Computer Investigative Specialists, Forensic Procedures URL*:* http://cops.org/forensic_examination_procedures.html (1999)

(7) Unknown , "GetTime" , New Technologies Inc. Forensic Software URL:http://www.forensics-intl.com/gettime.html (2000)