

TOWARDS HIPPOCRATIC LOG FILES

Andrew Rutherford¹, Reinhardt Botha² and Martin Olivier³

^{1,2}Department of Business Information Systems, Port Elizabeth Technikon, South Africa

³Department of Computer Science, University of Pretoria, South Africa

¹arutherf@petech.ac.za, +27 41 5043314, Private Bag X6011, Port Elizabeth, 6000

²rbotha@computer.org, +27 41 5043669, Private Bag X6011, Port Elizabeth, 6000

³www.mo.co.za

ABSTRACT

The World Wide Web (WWW) is fast becoming the central location for goods, services and information. The very factors that make the Internet such a powerful medium combine to make the Internet a treasure trove of personal information regarding individual Web users. This has led to internet users voicing concerns over the loss and violation of privacy. Inspired by the Hippocratic Oath, Agrawal, Kiernan, Srikant, and Xu (2002) introduced the concept of Hippocratic database systems. A founding tenet of such systems is that they should be responsible for the privacy of data they manage. Ten principles of Hippocratic database systems have been defined. The primary focus of this paper is to determine to which extent these same principles can be applied to log files. Once this is done, an architecture for the implementation of Hippocratic log files is introduced and discussed.

KEYWORDS

Computer Forensics, Hippocratic Databases, Internet, Intrusion Detection, Log Files, Personalization, Privacy, World Wide Web

⁰This material is based upon work supported by the National Research Foundation under Grant number 2054024 (Olivier) and Grant number 2050802 (Botha and Rutherford). Any opinion, findings and conclusions or recommendations expressed in this material are those of the author(s) and therefore the NRF does not accept any liability thereto.

TOWARDS HIPPOCRATIC LOG FILES

1 INTRODUCTION

“For the dynamic, pervasive computer environments of the future, give end-users security they can understand and privacy they can control” (Computing Research Association, 2003)

Internet users have rated a loss of privacy as their number one concern when transacting on the Web (Tavani, 1999). Various internet techniques and technologies can be used to erode user privacy. These include cookies, web bugs, spyware, banner ads and of course, log files. In general terms a log file stores information about user activity without the user expressly providing the information. This is perhaps the great area of concern, i.e. that users often have no idea their information is being logged, and even if they do, they may not be at all sure what information is being logged.

The Internet has become a focal point for information logging. Every action a user makes on the Internet is logged somewhere. The logged information may not, on its own, reveal the identity of an individual, but it may never the less be of a sensitive nature for example, user behaviour and interests. Various log files exist, for example Web server logs, proxy server logs and firewall logs. The logs may differ from business to business or indeed from Web site to Web site. Most Web sites will at a minimum log the following in their web server logs: IP address that initiated a request; date and time of the request; requested object; size of the requested object; request status code; size in bytes of the requested object; referring URL; and the browser version and platform (Pitzek, 2001). If a user had entered into a site from a search engine, then the referring URL log entry would not only contain the search engine URL but also the search criteria that the user used (Fotheringham, 2004).

User privacy concerns are by no means limited to the Internet. Inspired by the medical Hippocratic oath, Agrawal et al. (2002), introduced the concept of Hippocratic databases. Such databases should be responsible for the privacy of data they manage and are governed by ten key privacy principles. These ten principles are rooted in the eight data protection principles laid down by the OECD (Organization for Economic Co-operation and Development, 1980). The goal of this paper is to consider to what extent the ten Hippocratic principles can be applied to log files. In so doing the privacy concerns users' have with regards to log files, can begin to be addressed. In keeping with the spirit of the original paper on Hippocratic databases, various issues - as they relate to log files - will be introduced and discussed, without providing specific answers or solutions. We propose an initial design for maintaining Hippocratic logs. Much like the original Hippocratic strawman design, our design is aimed at raising relevant issues rather than provide a final design.

The remainder of the paper is structured as follows. Section 2 provides more information on how log file information can be linked to an individual, as well as means which users can implement to maintain a degree of anonymity. Section 3 provides insights into the reasons for information logging. Section 4 will examine and discuss each principle of Hippocratic databases in terms of its applicability to log files - a table summarizing the findings is provided. Section 5 introduces and explains a proposed high level architecture for Hippocratic log file implementation. Section 6 concludes this paper.

2 BACKGROUND

The information most commonly logged by Web servers was mentioned previously. Judging from what is logged, the only information, that could link back to an individual, is the IP address. Most people surf the Internet using an ISP, or from their place of work, quite possibly going through a proxy server. In such cases the IP address would be one assigned by the ISP or that of the proxy server itself. The question that then arises is, “can the user be personally identified by the information in the log files?”

In several scenarios this may indeed be so. A cookie could previously have been placed on the user's machine. In such a case the information in the log can be linked to an individual, or at the very least to a particular PC. It is also possible for a user to have filled in online forms for site registration, thus allowing information gathered directly (forms) to be linked with information gathered indirectly (logs) (Tavani, 1999). It must also be remembered that Internet Service Providers (ISPs) and proxy servers also collect log files. Thus not only can user activity be recorded at a destination site, but also at the point of origin. A log at the point of origin on a proxy server log, for example, can include the user name of the user - truly personally identifiable information.

Various tools and technologies exist that can provide users with anonymity while transacting on the WWW. Users may subscribe to a service known as anonymizer (Cranor, 1998). Subscription to this service allows all users' HTTP requests to be routed to a proxy based anonymizer, before submission to the destination site. Thus, with the proxy acting as a middleman as it were, no user information is received by the contacted Web site. Another means to maintain anonymity is based on the idea that "people can be anonymous when they blend into a crowd" (Cranor, 1998). Geographically dispersed users are collected into a group called a "crowd". All of a user's requests are forwarded through the crowd. When a member of the crowd receives the request, they can either submit it to the destination server, or to another randomly selected member of the crowd. By the time the request reaches its final destination it is impossible for the destination server, or for that matter any of the other crowd members, to determine which member initiated the request (Reiter & Rubin, 1999; Cranor, 1998). In this manner anonymity is assured. A decided drawback of privacy enhancing technologies is that they place the responsibility of preserving privacy and anonymity squarely on the doorstep of users. Additionally the technologies require a fair deal of understanding on the part of these users. While users do have genuine privacy concerns there are valid reasons for the logging of information, as addressed in the next section.

3 REASONS FOR LOGGING INFORMATION

Initially, the primary purpose of log files was to measure server load for diagnostic and planning purposes. However network connectivity, the Internet and e-commerce have supplied additional reasons for the logging of information.

3.1 Intrusion Detection and Computer Forensics

Due to the continued growth of internet popularity, millions of people are now online. By creating a web presence a company may expose its internal network to these self same millions. If only one percent of these users have malicious intentions, the security implications are substantial (Belgers, 1996). In many ways log files can be equated to an aeroplane's "blackbox", by the manner in which they provide a record keeping of system and network activity (Sarma & Mohirikar, 2003). Connection to the Internet has forced most companies to implement firewall technology. Firewalls can also provide important logging and auditing functions, for example, logging the kinds and amounts of traffic passing through the network (Curtin & Ranum, 2000; Sarma & Mohirikar, 2003). Intrusion detection systems can make use of log file information as a data source, allowing them to identify tampering or malicious activity within a system. Once such activity is discovered, the log can provide valuable information such as the time of the attack, geographic location of the intruder and the break in-route of the intruder. (Thomas, 2000; Gonzalez, 2003).

3.2 Monitoring Employee Activity

The monitoring of employee activity is a contentious issue. The number of employees with internet access has grown substantially in recent times. Along with this growth have come problems of decreased productivity, illicit communication of company secrets, and the accessibility to inappropriate material such as pornography (Nicolai Law Group P.C., 2001). Thus privacy implications aside, employers have many valid reasons for using log file information to monitor employee activity. "Just as

deadbolts and sophisticated alarms don't do much good if the thief is already inside the house, having computer network firewalls without monitoring employee activity can be equally ineffective inside the workplace" (Somerville, 2002). Actions taken by employees in misuse of the company network have definite implications for their employers. These implications may be legal, for example downloading pirate software, or economical, for example using valuable company bandwidth for music streaming (Somerville, 2002).

3.3 Statistical Analysis

It goes without saying that any company giving itself a web presence wants to attract visitors to their site - be this for reasons of e-commerce, or purely for the purposes of conveying their message to a larger audience. In order for a company to determine how effective its site is, it will need to track and measure their results. The web server logs capture valuable information that can be analyzed using a log file analyzer. The information that such an analysis yields includes, most requested pages, least requested pages, top entry page, top exit page, single access pages, top referrer, search strings leading to a site, conversion rate of visitors to buying customers, and errors, such as links to non-existing pages. Only once it is known how visitors act on a site will it be possible to make the changes necessary to make the site more effective (Bailey, 2000; Internet Marketing Engine, 2001). Statistical analysis need not require the use of personally identifiable information. Its major purpose is gaining an overall impression of the effectiveness of a Web site and pages within the site.

3.4 Web Site Personalization

E-business continues to grow and likewise the competition amongst players in this arena increases. Personalizing the web experience for individuals holds great potential in winning new customers and increasing existing customer loyalty (Mulvenna, Anand, & Buchner, 2000). Personalization involves using information known about the user of a Web site, to customize that site to better suit his needs or preferences. Thus personalization requires the creation of user profiles, and Web log files provide an additional information source for the development of profiles. In addition, patterns in user navigational behaviour may be discovered, by applying data mining techniques to log file information (Eirinaki & Vazirgiannis, 2003).

From the foregoing it is clear that information is being, and will continue to be logged. The challenge is to ensure that any personally identifiable information collected remains private. Agrawal et al. (2002) introduced the concept of a Hippocratic database as one in which the responsibility for the privacy of data it manages, be its founding tenet. The foundation of such a database is based on ten principles inspired by various privacy regulations and guidelines. These principles specify how such a database is responsible for the private information under its control. They also explain to any donor of private information what they can expect from this kind of database.

4 HIPPOCRATIC LOG FILES: THE PRINCIPLES

This section will address the applicability of Hippocratic database principles to log files by discussing each of the ten principles in turn. Each principle as laid down by Agrawal et al. (2002) will appear in italics, with the word "database" substituted with words "log file". Following the principle will be a short discussion of the applicability of the principle to log files.

4.1 Purpose Specification

For personal information stored in the log file, the purposes for which the information has been collected shall be associated with that information. There should be no problem in mapping this principle to log files. As stated previously in this paper there are a variety of reasons why information logging takes place. Associating these reasons with the personally identifiable information collected in log files does not seem to pose a problem.

4.2 Consent

The purposes associated with personal information shall have consent of the donor of the personal information. This is an admirable goal, and where possible the logging of personal information should adhere to it. However, there are reasons for logging information which supersede the right of the individual to consent to information collection - for example, intrusion detection and computer forensics. In the interests of openness and honesty, the fact that this logging is taking place, should be communicated to the user. Users can and should however, be afforded the opportunity to provide consent for other purposes of information collection. For security reasons, a user will be logged while they are deciding whether or not to provide consent to these other purposes.

4.3 Limited Collection

The personal information collected shall be limited to the minimum necessary for accomplishing the specified purpose. As stated previously certain purposes for information collection override the users' right to consent. When collecting information for intrusion detection and computer forensic purposes the "minimum necessary" may indeed be as much as possible. One can argue that this still meets this principle's requirement, albeit that for this particular purpose the minimum information required is as much as possible. At this juncture it is important to stress that collection of information is a separate issue to the use of information, as addressed by the next principle.

4.4 Limited Use

The log file shall only permit queries that are consistent with the purposes for which the information has been collected. A maximum amount of information may have been collected about a particular user for intrusion detection and computer forensic purposes. That information may not be used, say for statistical analysis, if the user has not given his consent to such usage. In this way the principles of limited collection and limited use, as they apply to log files, can operate harmoniously. This particular principle will, however, place certain requirements on the manner in which log files are stored. Log files should not be stored as un-encrypted plain text. Doing so would make it too easy for anyone with a text editor to view the information. Encryption is required since not all logged information is equally sensitive. An IP address, for example, has a much higher degree of sensitivity than the date of access. Additionally log files need to be stored in locations that facilitate and enforce proper access controls. Access controls will need to ensure that only persons with the required access rights, are granted access to log file information. Only in this manner can it be ensured that access to the log file take place in accordance with the purpose of the information and the consent to use that information provided by the user.

4.5 Limited Disclosure

The personal information stored in the log file shall not be communicated outside the log file for purposes other than those for which there is consent from the donor of the information. This principle overlaps with the principle of limited use - as disclosure of information, goes hand in hand with the use of information. Once again, for this principle to be met, the issues raised in the previous subsection need to be addressed, i.e. encrypting log file information and maintaining strict access controls to log information. During the course of a forensic investigation it may be required to disclose personal information, for example, the IP address of a potential intruder. In terms of tracing offenders this seems reasonable. However, once the information is in the hands of a third party, they may use it for a purpose other than the one originally agreed to by the user.

Persons involved in computer forensics possibly need to undergo specialized training. This training might include the taking of an oath, prohibiting the disclosure of personal information other than for forensic purposes. Violation of this oath could result in the offender no longer being able to practice as a forensic professional. Another area that needs to be addressed is the scenario where a log file must be examined by law enforcement officials, for example, tracing of a security offender.

In the process of this security investigation they may discover criminal activity unrelated to the initial security investigation. In most legal systems this evidence would not be admissible in court. This implies that the purpose for which access to log information is sought be clearly noted.

4.6 Limited Retention

Personal information shall be retained only as long as necessary for the purposes for which it has been collected. When addressing intrusion detection and computer forensic issues, it may not be possible to specify an exact length of time for which the information is to be retained. However, the retention period should be reasonable. It has been stated that for security reasons, user information must be logged - even during the time when they are deciding whether or not to provide consent to other information collection purposes. In the spirit of Hippocratic databases, such information shall be used for forensic purposes only, and will therefore be retained for a very short period.

For other purposes of information collection, where the user has consented to the use of information, the retention period can indeed be limited and information purged once the purpose of collection has been achieved. For purposes of statistical and trend analysis it may be required for information to be retained for extended periods of time. However, information can be aggregated and summarized, for example by no longer storing information on each page hit, but merely the total number of page hits. This aggregated information can then still be stored and used for statistical and trend analysis.

In the event that information is not summarized, it can be sanitized of personally identifiable information, once the reasons for needing this information have expired, for example, removing the IP address from all log records. Limited retention will be very closely linked to the principle of purpose i.e. the purpose for which information is collected will govern the retention period.

4.7 Accuracy

Personal information stored in the log file shall be accurate and up-to-date. This principle as it applies to log files is a non-issue. Databases require the manual entry of information by humans. In such cases human entry errors will always be a concern. Log file information collection, on the other hand, is an automatic, machine driven process and the same concerns of data accuracy do not apply, and hence data accuracy is unimpaired. It must be remembered, however, that a machine will accurately record the information it receives, but has no way of verifying that this information is correct.

4.8 Safety

Personal information shall be protected by security safeguards against theft and other misappropriations. The safety principle overlaps with at least two other principles, namely limited use and limited disclosure. In order for the safety principle to be met, previously raised issues need to be addressed i.e. log files may need to be encrypted and access control mechanisms need to be in place to enforce users' privacy preferences.

4.9 Openness

A donor shall be able to access all information about the donor stored in the log file. The issue that needs to be addressed here, is the degree of openness that is required as it applies to log files. Should the information that is collected for intrusion detection and computer forensics purposes be open for the donor to see. This would give the opportunity for intruders into the network, to view what information regarding their activities have been stored. This may then give them the opportunity to attempt to cover their tracks before any intrusion is detected. Once again this highlights the need for the format in which log files are stored and accessed to be addressed. If all information regarding an information donor is open for his inspection, then mechanisms must be in place to ensure that this information cannot be deleted or altered.

The information collected for purposes to which the user has consented, does not pose the same concerns as forensic information. Such information should be open for inspection. The ability of users to access log files raises a question - should such user access itself be logged? It has already been motivated that the information in the log file will be accurate due to the machine driven nature of its collection. Thus user inspection would serve the purpose of checking to see what information is stored and not for reasons of checking accuracy.

4.10 Compliance

A donor shall be able to verify compliance with the above principles. Similarly the log file shall be able to address a challenge concerning compliance. Ensuring that the principle of compliance is met, raises new issues and challenges. A log file provides an audit trail of what has transpired on a system or network. This raises the question of whether one needs a log file to maintain an audit trail of accesses to that log file. What information would such a log file contain? If this audit log file contains personally identifiable information, will we once again need user consent for its collection? Another possibility is for log files to be stored by a party trusted by the information donor and the information collector. The role of this third party would be to ensure compliance to the principles of Hippocratic log files. The involvement of a third party in the process will itself raise new areas of concern, for example, if the connection to the third party is interrupted, then information that is required for security and forensic purposes will not be captured.

Table 1 summarizes this paper’s findings. Each row of the table contains a principle followed by a compliance indicator. A ++ indicates potential full compliance. A + indicates potential compliance, subject to limitations due to security and forensic purposes of log files. A - indicates that a principle is a non-issue. A ++* indicates potential full compliance, provided technical issues regarding the manner in which log files are stored and accessed are addressed.

Table 1: Hippocratic Log File Compliance

Principle	Compliance
Purpose Specification	++
Consent	+
Limited Collection	+
Limited Use	++*
Limited Disclosure	++*
Limited Retention	++
Accuracy	-
Safety	++*
Openness	+
Compliance	++*

5 HIPPOCRATIC LOG FILES: IMPLEMENTATION ARCHITECTURE

Figure 1 represents a high level overview of a possible implementation of Hippocratic log files. This architecture was designed to conform to the principles of Hippocratic logs. A solid line indicates actions that will occur. A dashed line on the diagram indicates an action that may occur, depending on user choices.

Users initiating requests would first be routed to an “unlogged” server which performs limited logging - this is indicated by the (A) of Figure 1. The logs maintained by this server will be of a

very temporary nature, for example, 24 hours. The idea of utilizing a completely unlogged server was considered, but rejected due to possible security implications. At this “unlogged” server, users will be informed that the logged server logs personal information for the purposes of security and forensics. It can be made clear to them that information collected for security reasons will only be used for security related purposes. Any other reasons for which collected information may be used, should be made clear. At this point users have the opportunity to terminate communication. Due to the temporary nature of the logs on this server, any information they released will be discarded. This ensures compliance to the Hippocratic principle of consent.

As stated previously in this paper, a user may be logged when initiating a request either from their place of work, or through an ISP. In such cases employers should inform employees of company logging policies and ISPs should do the same for their subscribers.

The (B) of Figure 1 indicates that users choosing to proceed, may set up their privacy preferences. These users will at this stage be informed of all the purposes for which the site is collecting information. They can then choose whether they agree to the use of their information, for each collection purpose. This again enforces the principle of consent. To avoid the scenario of frequent users having to re-enter preferences, cookies might be used to recognize returning visitors. In such a case a user can be directly routed to the logged server - indicated by (C). Users should, however, always have the option of changing their preferences.

(C) and (D) indicate a user being routed to the main server. By this time a user has agreed to the logging of information, and has set up his privacy preferences. All activity occurring on the logged server is recorded to the log file indicated by (E). All personal information that is logged will contain the purpose/s for which it is logged, thus adhering to the Hippocratic purpose principle.

The (F) of Figure 1 shows a request for log file information. Such a request could be from within the organization itself, or potentially from a user whose information has been collected. The degree of openness given to users, with regards to log file information, raises several questions. In the first instance, should users be granted access to this information? Secondly, if access is granted, should access not be controlled by an additional server maintaining a copy of the log file? Thirdly, should all user accesses to the log be themselves logged? An alternative to allowing users full access to the log file is to allow them access to the audit log only. In this way they may not see what information is stored, but will be able to see that their information was accessed, and for what purpose.

Questions of openness aside, all requests, as indicated by (F), would pass through a log query processor. Part and parcel of the query processor’s responsibilities would be to enforce access control mechanisms. These mechanisms will verify that the person requesting access is authorized to view the information. They will also ensure that the information returned or accessed, be restricted to those users who have consented to its use. By maintaining strict access control, adherence to the principles of limited use, limited disclosure and safety can be ensured.

All attempts to access the log file, successful or unsuccessful, should be logged to an audit log, as indicated by (G). Logging these accesses will aid in the enforcement of Hippocratic principles; particularly the principle of compliance. Information contained in the audit log will provide a history of who has accessed, or attempted to access, the log file. The purpose for which the log file was accessed will also be recorded. If access requirements are fulfilled, access to the log file/s will be granted - indicated by (H). The audit log can be referred to if ever questions of compliance to Hippocratic principles are raised.

6 CONCLUSION

Logging of personal information is a definite privacy concern for the owners of personal information. It has however been established that, particularly for reasons of security and computer forensics, information logging must take place. To alleviate user concerns, means need to be developed to

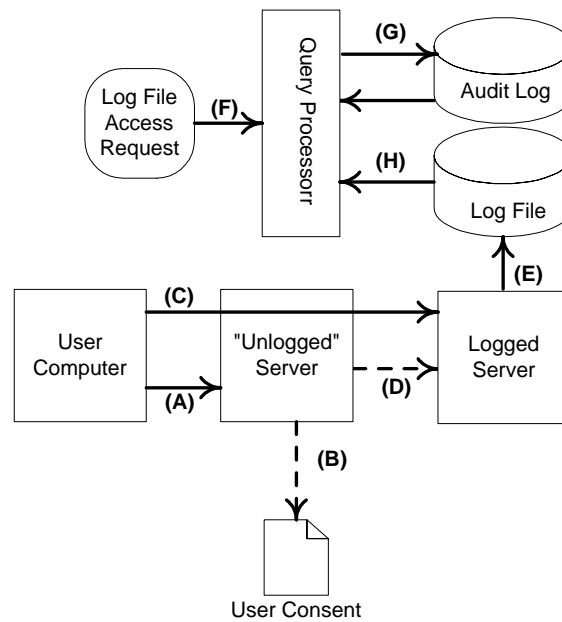


Figure 1: Hippocratic Log Architecture

minimize the privacy impact that this information holds. This can be achieved by giving users more control over their information. They may not be able to control its collection, but they can indeed have greater control over its use.

This paper examined the application of Hippocratic database principles to log files as one means of providing users with such control. Each of the ten Hippocratic principles were discussed in turn. These discussions raised several issues, relating to log files, requiring resolution. These issues primarily revolve around the format in which log files are saved; plain, un-encrypted text is not a viable option. In addition the access control mechanisms to log file information must ensure and enforce user privacy preferences.

This paper further proposed a high level architecture for Hippocratic log file implementation. This architecture serves a similar purpose to the original Hippocratic database strawman design i.e. it is not meant to be a final design, but to raise relevant issues and questions. Further investigation and research is required to further refine and develop this architecture.

7 REFERENCES

- Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. (2002). *Hippocratic Databases*. Available from: http://www.almaden.ibm.com/software/dm/Hippocratic_Databases/index.shtml. (Last cited:01 Apr 2004)
- Bailey, D. (2000). *Log File Issues*. Available from: <http://slis-two.lis.fsu.edu/~log/issues~1.htm>. (Last cited:01 Apr 2004)
- Belgers, W. (1996). *Firewalls - an Introduction*. Available from: <http://www.surfnet.nl/innovatie/desire1/deliver/WP5/D5-1.html>. (Last cited:01 Apr 2004)
- Computing Research Association. (2003). *Four Grand Challenges in Trustworthy Computing*. Available from: <http://www.cra.org/Activities/grand.challenges/security/slides.pdf>. (Last cited:15 Apr 2004)
- Cranor, L. F. (1998). Putting it together: Internet privacy: a public concern. *netWorker*, 2(3), 13–18.

Curtin, M., & Ranum, M. (2000). *Firewalls FAQ*. Available from:<http://www.faqs.org/faqs/firewalls-faq/>. (Last cited:01 Apr 2004)

Eirinaki, M., & Vazirgiannis, M. (2003). Web Mining for Web Personalization. *ACM Transactions on Internet Technology (TOIT)*, 3(1), 1–27.

Fotheringham, J. (2004). *A Web server log file sample explained*. Available from:http://www.jafsoft.com/searchengines/log_sample.html. (Last cited:01 Apr 2004)

Gonzalez, A. (2003). *Intrusion Detection Systems: An Introduction*. Available from:http://www.linuxsecurity.com/feature_stories/feature_story-143.html. (Last cited:01 Apr 2004)

Internet Marketing Engine. (2001). *How to read Web server log files*. Available from:<http://internetmarketingengine.com/how-to-read-server-log-files.htm>. (Last cited:01 Apr 2004)

Mulvenna, M. D., Anand, S. S., & Buchner, A. G. (2000). Personalization on the Net using Web Mining. *Communications of the ACM*, 43(8), 122–125.

Nicolai Law Group P.C. (2001). *Technology Use Policies*. Available from:<http://www.niclawgrp.com/memos/200112.html>. (Last cited:01 Apr 2004)

Organization for Economic Co-operation and Development. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available from:http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1%_1,00.html. (Last cited:09 Jun 2004)

Pitzek, S. (2001). *Security - Privacy on the Internet*. Available from:http://www.vmars.tuwien.ac.at/courses/akti12/journal/01ws/article_01ws_Pitzek.pdf. (Last cited:01 Apr 2004)

Reiter, M. K., & Rubin, A. D. (1999). Anonymous Web transactions with Crowds. *Commun. ACM*, 42(2), 32–48.

Sarma, S., & Mohirikar, N. (2003). *Logs and Forensics*. Available from:<http://www.cert-in.org.in/presentation/Logs-Forensics.pdf>. (Last cited:01 Apr 2004)

Somerville, L. (2002). *Seeking Security Within*. Available from:<http://triad.bizjournals.com/triad/stories/2002/07/22/focus1.html>. (Last cited:01 Apr 2004)

Tavani, H. T. (1999). Privacy Online. *ACM SIGCAS Computers and Society*, 29(4), 11–19.

Thomas, B. (2000). *Intrusion Detection Primer*. Available from:http://www.linuxsecurity.com/feature_stories/feature_story-8.html. (Last cited:01 Apr 2004)

A. Rutherford, R. A. Botha, and M. S. Olivier, "Towards Hippocratic log files," in *Proceedings of the Fourth Annual Information Security South Africa Conference (ISSA2004)*, Midrand, South Africa, June/July 2004. Published electronically.

©The authors

Source: <http://mo.co.za>