4

A TOP-DOWN APPROACH TOWARDS TRANSLATING ORGANIZATIONAL SECURITY POLICY DIRECTIVES TO SYSTEM AUDIT CONFIGURATION

Atif Ahmad, Tobias Ruighaver
University of Melbourne

Abstract: There is a significant gap between the stated objectives of organizational security found in corporate security policy and the audit configuration of event logs present on IT systems. Audit configuration has always been a bottom-up process. As a result, the design and implementation of audit configurations is often constrained by the audit management interface that often models operating system structures rather than real world behavior. This paper argues for a top-down approach in the establishment of IT audit policies and practices. We propose that management should develop an organization wide audit policy that will set mandatory audit directives and ensures that the audit configuration reflects the needs of the organization as defined in the security policy.

Key words: audit policy, security, logs

1. INTRODUCTION

In the past, IT security in the corporate environment has primarily been the responsibility of systems administration [NePa89]. As the main threat against systems was perceived to be external intrusions, audit logs played an important role since they are the primary source of intrusion related information [VacLie89]. Originally, the main use of audit logs was to monitor performance or detect intrusions originating from an external source [Anderson80]. Most security measures undertaken were predominantly independent of the corporate security policy, which was either nonexistent or

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

provided inadequate guidance in setting up and maintaining security and audit configuration for IT systems.

With the passage of time however, the term "intrusion" has begun to express a wider meaning closely related to security policy. Any violation of the security policy is now classified as an intrusion. Security policies have become more comprehensive and frequently include guidelines addressing acceptable behavior. Developments in internet connectivity highlighted the importance of using audit logs to detect violations of security policy and more recently to collect forensic data to support organizational security objectives [Sommer97].

Audit configuration has traditionally been a bottom-up process. Audit management tools have unfortunately constrained the design and implementation of audit configurations due to their modeling of operating system structures rather than real world behavior. In this paper we advocate a top-down approach, starting with organizational security objectives working down to an organization wide audit policy. This approach ensures that audit configuration across the organization is consistent to some degree, and supports the organization's security objectives. We suggest the use of an organization wide audit policy specifying mandatory audit directives that support the organization's security objectives. A distinction will be made between the gathering and management of audit data. This distinction will be the foundation of a three phased model used to describe the auditing process.

2. AUDIT CONFIGURATION AND POLICY DIRECTIVES

The gathering of audit data has not remained focused on organizational security objectives due to the lack of guidance from security policy on the precise requirements of audit data collection.

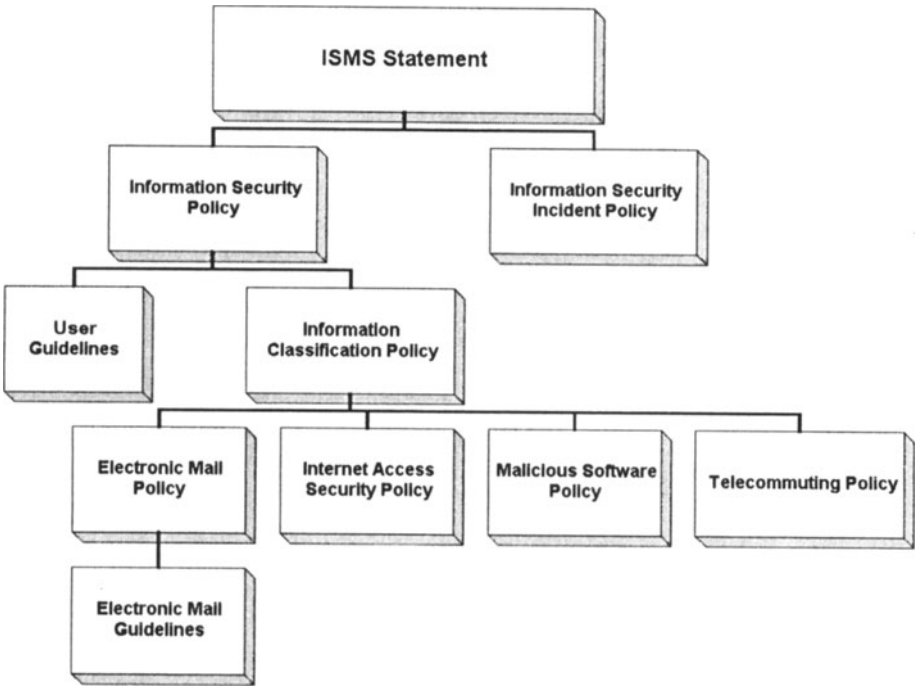

Figure 1. A typical example of the security policy of a large-scale information security conscious corporation

As an example we will look at the structure of an extensive security policy of an existing large-scale corporation. We selected this example because it is a typical sample of security policies of such organizations.

Despite the implied depth and coverage of the above structure, there is little guidance to security administrators as to what audit data must be collected at a minimum. In addition, there is no clear indication of the existence of any associated documentation that may provide more information relevant to audit. In the above policies the following references to audit data exist:

Information Security Policy
5. Global Security Environment
(5.3 Monitoring)
5.3.2 All records pertaining to security related events shall be reviewed and retained.

Local Security Environment Resources
(6.3. Access Control)
6.3.2 Access control records shall be maintained and reviewed periodically.

7. Electronic Security Measures Resources
(7.3 Access Control)
7.3.5. Access to and from external resources shall be strictly controlled and monitored

Internet Access Security Policy
4. Policy
4.1.3. XXX shall log Internet use. XXX staff visiting a site deemed inappropriate in accordance with this policy shall be subject to disciplinary action.

The above statements are the only guidance available to system administrators on the audit requirements within the corporation. As a result there will be a significant gap between the stated objectives of organizational security found in corporate security policy and the audit configuration of event logs present on systems. Although systems administrators are assumed to be responsible for the formulation of system and network-based configuration, the translation of relevant security objectives to system audit configuration has not been straight-forward. It is frequently inaccurate and incomplete resulting in insufficient data being collected and incorrect selection of relevant data needed to support organizational security objectives.

To further complicate this process, security policies are beginning to require the collection of forensic data for the purposes of litigation. The main aim of security policies is to prevent intrusions where an intrusion is defined as a violation of security policy rather than just an attack originating from an external source [Anderson80]. Recently audit data is being viewed as a potential source of evidence in legal proceedings [Sommer98].

However, administrators generally do not retain the knowledge necessary to determine which sets of data must be selected to support the need for forensic data collection [Sommer92]. Furthermore, the process by which data is collected and preserved must meet strict guidelines to be admissible in court. These guidelines are known to specialists in this field but most administrators are not trained in issues related to the gathering and preservation of forensic data.

3. A TOP DOWN APPROACH TO THE DEVELOPMENT OF AN AUDIT POLICY

To reduce the gap between organizational security policy and audit configuration and to align the gathering of audit data with the organizational

definition of "intrusion", an organization wide audit policy is needed (fig 2). We suggest the establishment of set mandatory audit directives that support the organization's security objectives and ensure that the security of systems will reflect the needs of the organization as defined in the security policy. These directives must stipulate the gathering of data for intrusion detection and/or forensic purposes. Other organizational needs, like the collection of data for performance monitoring, may also be included in the audit policy. The aim of such a document is to provide administrators with a defined audit policy that can then be used to design audit configurations for various IT platforms, thereby maintaining consistency across the IT domain.

Our research on information security policies reveals that it is uncommon to find a high-level audit policy applicable across the various IT platforms within an organization. Organizational security policies are typically the only guidance endorsed by management available to the administrators who are responsible for IT security. Administrators are in a better position to design an accurate audit collection scheme from existing IT infrastructure if they are provided a high-level audit strategy guide. Such guides provide administrators with a mapping between organizational security directives and system strategies for audit gathering and managing. It is important to note that there remains the difficulty in implementing system strategies using the currently available audit management tools provided by operating systems designers. This paper concentrates on the high level audit policy but recognizes that current audit management technology may not allow resulting system strategies to be implemented conveniently.

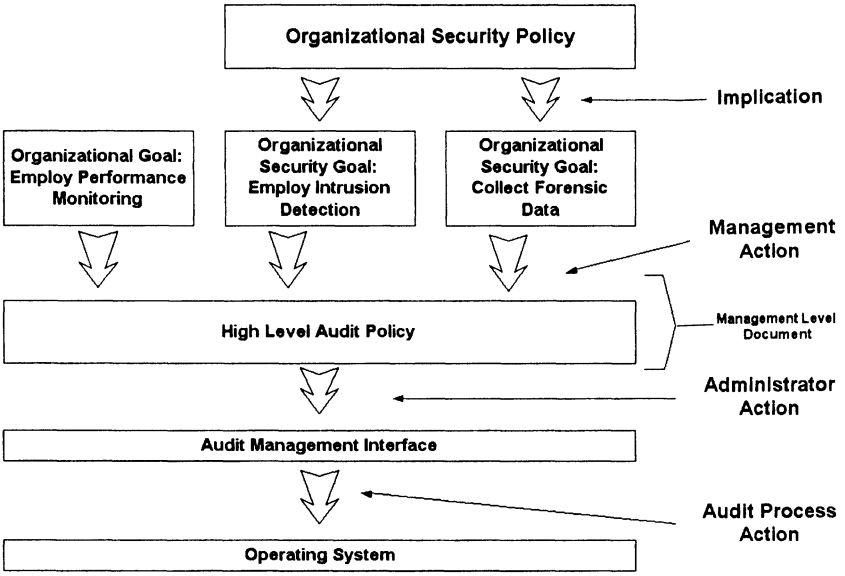

Figure 2. A Mapping between Organizational Security Objectives and System Strategies for Audit Gathering and Managing

4. ISSUES TO BE ADDRESSED BY A HIGH LEVEL AUDIT POLICY

We are currently developing an extensive framework of issues that have been highlighted by experts involved in auditing processes and theory. In this section we present some issues that are fundamental to auditing and must be addressed in the development of an audit policy as part of the top down process described previously.

An audit policy must specify the types of data that must be collected to ensure that organizational security objectives are being met. In addition, any compression and security measures to protect audit data from its generation to its final deletion must be addressed. The lengths of time that various types of audit data sets must be kept should also be stipulated and storage issues especially the precise location as to where the data will reside.

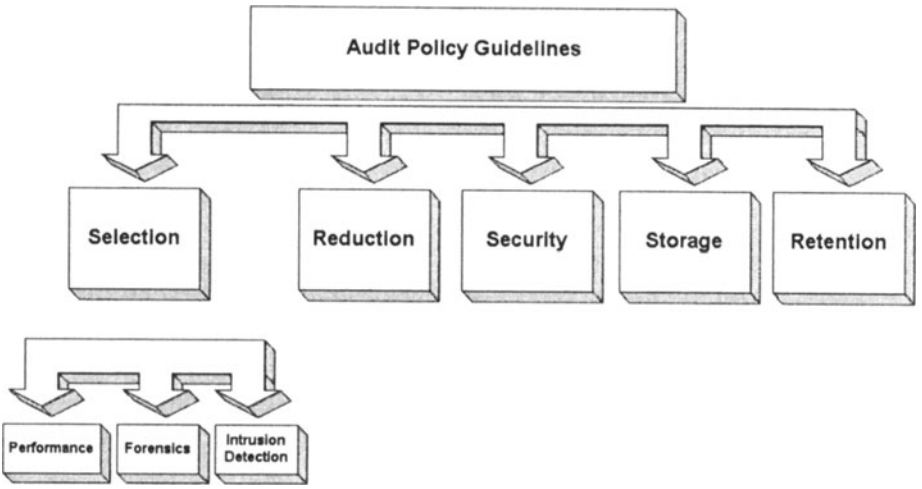

Figure 3. Essential Components of a High-Level Audit Policy

4.1 Selection

The selection of events that is audited should be based upon the organizational objectives as set by audit policy guidelines. Audit events related to performance, forensics and intrusion detection are possible examples. Audit trails that are designed with the company's objectives in mind tend to have a higher concentration of useful data.

There are a number of issues that relate to the selection of a minimum set of audit data that fulfils stated objectives. For example, audit events may not provide sufficient context without related files [Schaen91]. Audit events may lack sufficient detail, and the logs may not identify the real world incident in any useful way [Sommer98].

In general, there are few audit security policies that specify the kinds of data that must be logged for each event. However the following have been mentioned in security policies [ACSP98]:

- Time and date of activities
- User ID
- ID of local terminal or remote computer
- System job number/process number
- Error conditions like failed attempts at executing a task

4.2 Reduction

Frequently audit trails become extremely lengthy largely due to the presence of data irrelevant to the security incident. There is a tendency to filter or reduce data in order to focus on more significant data, however it may be difficult to prove the neutrality of such filteration processes[Sommer98]. Guidelines are necessary to prevent unauthorized reduction that may affect integrity and therefore admissibility of audit data in court.

4.3 Security

Security issues affecting audit trails include the confidentiality, integrity and availability of audit data to the organization [Schaen91]. Access control may need to be enforced on collected audit data to prevent unauthorized access.

As a minimum a high level audit policy should discuss :

- Access control requirements on audit trails
- Organizational procedures on obtaining access to audit trails

4.4 Storage and Retention

Issues relating to the location of stored audit logs whether local or centralized. Separation between security levels of data must be taken into account as well as the impact of encryption on consolidation. Backup media itself must be protected and disposed off securely when retired [Scahen91].

Audit guidelines must stipulate the minimum retention period for sets of audit data. In addition, the possible elimination of one set of audit data may affect the usefulness of another must also be taken into consideration.

The statement below is a catch-all phrase that is frequently used in security policies but may not be sufficient to ensure that security administrators apply the same guidelines to audit data [ISP97].

"All backup media will be stored in a safe, secure environment, in accordance with the manufacturer's specifications. Media which has been used to store sensitive data will be disposed of securely and safely when no longer required."

Audit guidelines must state:

- The precise storage environment where audit data must be kept
- Whether audit data will be stored in a centralized location or distributed location

5. GATHERING, MANAGING AND ANALYZING AUDIT DATA

The selection of audit data to log is the central issue facing systems administrators. Audit data must reflect organizational security guidelines and must detect and deter security policy violations as well as providing evidence for forensic purposes. To collect audit data a distinction must be made between the gathering of a system's event data as opposed to the management of the audit data set required by the organization. For example a high-level audit policy may specify the characteristics of a minimum set of audit data that must be collected by the administrator. The characteristic audit data, its storage requirements, period of retention, security, and reduction may be addressed as part of the organization's management responsibility.

A specific platform used in the organization may not allow all such events to be conveniently collected through its audit management interface (fig 2). In such a case administrators must implement additional gathering mechanisms to attempt to satisfy management directives. Issues related to the gathering of audit data relate to what event data can possibly logged, where in the operating system this data can be securely and accurately extracted.

We found the distinction between the gathering and management of audit data (fig 3) helpful in illustrating the fundamental processes that makes up auditing in general. The first being the gathering of event data which involves deciding what kinds of data need to be collected and whether such data is available from existing auditing facilities. The management of data addresses the amount of data collected, how long it is stored, its security, and maintenance. Finally the analysis of data involves anomaly detection and other techniques of sifting through logs for relevant information.

These three fundamental phases of audit data collection are useful in emphasizing the distinction between audit management processes that must be independent of platform specifics as opposed to the audit gathering that is heavily reliant on the existing operating system and its audit facilities.

It follows that an organization-wide audit policy would be useful in serving as a set of guidelines for the development of an audit management process. In addition, a high-level audit policy makes the process of evaluating the suitability of audit configurations more efficient and accurate. Whereas correlating implied security policy objectives to audit configurations is a more complicated and error-prone process.

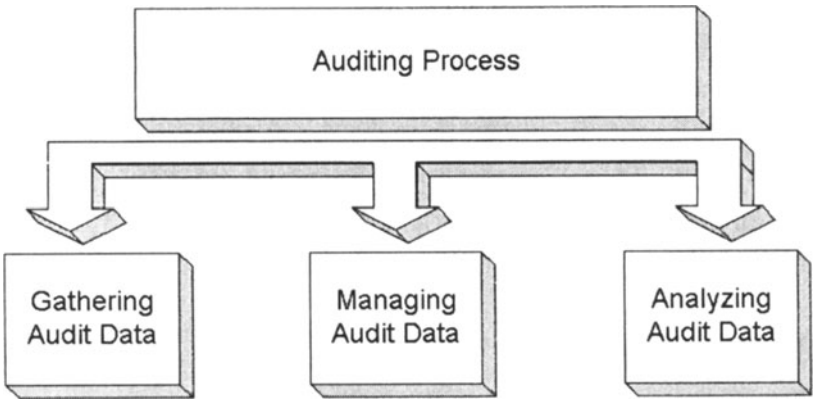

Figure 4. The Fundamental Phases of Audit Collection

6. CONCLUSION

The formulation of a high level audit policy will reduce the gap between organizational security directives and the audit configuration of event logs. In addition such an audit policy will bring uniformity to audit configurations across an organization's varied platforms.

We have collected a list of issues that are not addressed by most organizations when setting up event logging. These issues must be addressed by a high level audit policy.

Administrators may use organizational security objectives and the fundamental issues relating audit outlined in this paper to develop a high level audit policy relevant to their organization.

Although the breach between organizational security objectives and audit configurations will be somewhat reduced by a high level audit policy, it is important to note that implementing high level audit strategies remains difficult to implement through the use of currently available audit management tools.

7. REFERENCES

[ACSP98] Administrative Computing Security Policy, University of Pennsylvania, 1998.

[Anderson80] Anderson, J. P., *Computer Security threat monitoring and surveillance.* Technical Report. James P. Anderson Co., Fort Washington, PA, April 1980.

[Denning86] Denning, Dorothy, "An Intrusion-Detection Model", *From 1986 IEEE Computer Society Symposium on Research in Security and Privacy*, pp 118-31.

[ISP97] Information Security Policy, University of New South Wales, 1997.

[NePa89] Neumann, Peter, Parker, Donn, "A Summary of Computer Misuse Techniques", *Proceedings of the 12th National Computer Security Conference*, Baltimore, Maryland, 10-13 October, 1989.

[Schaen91] Schaen, S. I.,McKenney, B.W., "Network Auditing: Issues and Recommendations." IEEE: 66-79.

[Sommer92] Sommer, Peter, "Computer Forensics: an Introduction", *Compsec '92*, Elsevier, 1992.

[Sommer97] Sommer, Peter, *Downloads, Logs and Captures: Evidence from Cyberspace,* Journal of Financial Crime, October, 1997, 5JFC2 138-152;

[Sommer98] Sommer, P. "Intrusion Detection Systems as Evidence", *RAID 98*, Louvain-la-Neuve, Belgum.

[VacLie89] Vaccaro, H.S., Liepins, G. E., "Detection of anomalous computer session activity", *In 1989 IEEE Symposium on Security and Privacy*, pages 280--289, Oakland, CA, USA, May 1989. IEEE Piscataway NJ USA.

[Wee96] Wee, C.: *Policy Directed Auditing and Logging*, PhD Thesis, UC Davis, Dept. of Comp. Science, 1996.