11.2 Audit Requirements

An audit service must satisfy a set of requirements for both the service and the quality of service. The audit function is to analyze logs, audit trails or other captured information about an event, such as entering a building or accessing resources on a network, to find and report any indication of security violations. While each situation that calls for an audit is unique, there are common generic requirements that apply to all audit situations. This pattern provides a common generic set of audit requirements. The pattern also helps you to apply the general requirements to your specific situation, and helps you determine the relative importance of conflicting requirements.

Example

The museum's research department has a network that they use for messaging and collaboration with various universities around the world. Among the types of information exchanged and stored are details about the location of various gemstone mines. Every six months the museum must present a report of the information exchanges to the board of trustees. The museum wants to take six months' worth of activity and summarize it into the critical and non-critical events that occurred over that six month period, and who was involved in those events. Samuel the museum system engineer understands this goal, but at the same time he understands that capturing extensive audit information can degrade system performance and require significant resources for storage and analysis. Privacy considerations are also a constraint on the capture and use of audit data. Samuel needs to identify requirements for an audit service that will help the museum achieve the goals while balancing the constraints.

Context

Accounting requirements and their relative importance are understood, for example, from applying SECURITY ACCOUNTING REQUIREMENTS (360). The planned uses of audit are understood.

Problem

Audit is a security service that scrutinizes logs, audit trails or other captured information and attempts to discern more detailed information about an event. It analyzes the event information for any indication of security violations. You need a clear set of requirements to ensure that the audit strategy employed actually satisfies the needs

of the organization or system. Requirements for audit often conflict with each other, and trade-offs among them are often necessary. The conflict stated above in the example is that the need to provide an audit trail must be balanced with resource and privacy constraints. What types of information are appropriate or required for an audit system to analyze?

How can you determine a balanced set of specific requirements for an audit service, and their relative importance?

The process of selecting and prioritizing audit requirements needs to balance the following forces.

- Collecting extensive relevant audit raw data increases the likelihood of achieving the desired security properties, especially accountability.
- Collecting extensive audit raw data increases the risk of violating privacy laws, or of abusing such data, or of damaging the reputation of the collector.
- Applying audit has many associated costs (support personnel, software, additional processing time, and so on) that are counter to the organization goal of minimizing total costs.
- Audit errors can result in lack of accountability in two ways. If person A commits an act that violates security, and the audit concludes that person B committed this act, then (1) person A is not held accountable for his action, and (2) person B is incorrectly held accountable and suffers consequences for an act he did not commit.

Solution

Specify a set of audit requirements for a specific domain such as a system or organization, and determine the relative importance of each requirement. The solution has two aspects: a requirements process and a common set of generic requirements.

Requirements Specification and Prioritization Process

A system requirements engineer, in conjunction with an enterprise architect, typically perform the requirements process. An important first step is explicitly to define the domain for which you are specifying audit requirements, such as a specific system, or types of activities and events. You also define factors such as organization constraints that affect the specialization and importance of requirements. Then you specify audit requirements for the target domain, using the generic requirements provided below. The final activity is to define the relative importance of the specified requirements.

Generic Requirements Description

The audit function is to analyze logs, audit trails or other captured information about an event, such as entering a building or accessing resources on a network, to

find and report any indication of security violations. The following is a general set of requirements appropriate to an audit service.

- Provide information about malicious and unwanted events.

  An audit service must provide information about events that are actually or potentially harmful to the organization. The information is used to determine what the event was, when and where the event happened, and why and how the event happened. It is also used to determine where organization vulnerabilities exist, and help the organization determine how a threat may have become a reality. The circumstances of an undesirable event, including the location and time of day and date, should be captured. The location of the event needs to be included in the details so that planners and investigators of the event can examine the area for more clues about the event. Location might be physical, such as a building, room or gate, or 'virtual,' such as a network or a Web site. Other event information may include whether or not any elements of the attack were detected in advance, and responses that ensued. This requirement implies an ability to distinguish desirable or normal events from undesirable ones. Such a distinction is often not possible until after the data is captured and analyzed.

- Provide information that associates actors with events.

  An actor may be a person, or a hardware or software element. The audit service needs to provide information not only on events that occur, but also what actors were involved in the events. A minimum requirement is to provide actor identification. Other actor information may include the location of the actor during the event and role of the actor in the event. The information is used eventually to assign the responsibility of the event to the actors. Information on thwarted attacks will need to be fed back to security officers to ensure awareness about what does work.

- Provide information on actor activity over a period of time.

  Predicting behavior can be used to prevent malicious activity from harming the organization. Over the course of time users develop habits when using a system, and those habits can be gathered into a user profile. An audit system can be used to provide details of these habits to distinguish one user from another. This information can also be used to better understand the vulnerabilities in the system, and allow decision makers the opportunity to dictate what vulnerabilities should be addressed. Decision makers want to be sure that actors who engage in activity in the organization are performing their duty in a manner that does not violate or threaten security.

- Be able to determine what captured information is relevant.

  An audit usually takes place over an extended period of time. Audit also examines information about events that have been captured over an extended period of time. In order to identify security violations that have occurred over that

time, an audit activity must take care to examine the information carefully and thoroughly to ensure that the relevant information has been discerned from the captured events. Audit logs typically contain a large amount of captured information, but the information that pertains to an event of interest is by comparison very small. Finding the relevant information is often not an easy task. Sometimes even determining which events are of interest is not easy.

- Perform its service when needed.

  An audit system needs to be able to provide its services during times when the tracking of events is absolutely important, yet the ability to do so may be hampered by attacks. This requirement is essential to support availability, and concerns the readiness of the audit service.

- Provide reliable and accurate information.

  An audit system provides information relative to a specific event, and the user of the audit information wants to have confidence in the reliability and integrity of the information. Although audit was not responsible for capturing or storing the raw logging information that was input to the audit process, it may also need to provide information about the reliability and integrity of that information as well. Those working with the audit mechanisms must be trusted not to alter any information previously captured. In addition, any automated tools supporting the audit process need to be fully understood with regard to how they process the information and the rules used for establishing associations between disparate pieces of information. This requirement is essential to support integrity, and concerns the trustworthiness of the information the audit service provides.

An additional set of requirements applies to all service requirements patterns. Instead of duplicating the discussion of the same set in each requirements pattern, they are simply listed here, because they do need to be considered in each requirements pattern. The requirements are: minimize time and effort to use, minimize mismatch with user characteristics, risks to user safety, costs of per-user set-up, costs of maintenance, management, and overhead, and changes needed to existing system infrastructure. Further discussion of each of these cross-cutting requirements, including implementation factors, is given in I&A REQUIREMENTS (192).

The remainder of this pattern focuses on the audit-specific requirements identified and discussed above.

Implementation

This section first provides more detail about the process that was summarized in the Solution section, then discusses factors in determining relative importance of requirements.

Process Guidelines

The requirements process is typically performed by a system requirements engineer, in conjunction with an enterprise architect, and includes several steps:

1. Establish the domain for which the audit service is needed.

   Ensure that the domain has been identified and scoped: typical audit domains include information system, physical facility, network, portal, category of events, or entire organization. The domain consists of at least three parts: a defined scope of actors or users, a defined scope of assets, and a defined scope or set of events that involve actions or operations on those assets. Other constraints may bound the domain—for example, the audit requirements for a real-time service may differ from those for a multi-year service: these might represent two domains.

2. Specify a set of factors that affect the specialization and importance of requirements.

   The factors include use of audit, audit needs, organization constraints, and priorities. You can find a general candidate set of factors below.

3. Specify the audit requirements for the target audit domain.

   To do this, specialize the set of generic requirements given in the Solution section.

4. Define the relative importance of specific requirements.

Factors in Determining Relative Importance

Table 11.3 reiterates the generic requirements described in the Solution section, and identifies factors for judging their relative importance to an organization or system. For each factor, the table also indicates the resulting requirement priority, in terms of High, Medium, and Low.

Example Resolved

Samuel the museum systems engineer defines the museum's research network as an audit domain. Table 11.4 shows the requirements ratings Samuel has specified for this domain.

Known Uses

The general audit requirements and the process of specifying audit requirements described in this pattern are widely known, but are generally used informally, as opposed to being codified or published. The requirements as stated in this pattern represent a consolidation of MITRE Corporation's experience in working with multiple

Table 11.3 Audit service requirements factors

GENERIC REQUIREMENT	FACTOR	RESULTING PRIORITY
Provide information about malicious and unwanted events	Required by law or other mandate outside of the organization, or events involve highly-sensitive or valuable assets.	High
	Internal organization concern rather than external mandate, or events involve assets of medium value	Medium
	Only prevention approach used, not detection or response, or events involve low value assets.	Low
Provide information associating actors with events	Assigning responsibility is high priority, because it is required by law, or events involve highly sensitive or valuable assets.	High
	Accountability is an organization concern and not a legal or external mandate, or events involve assets of medium value, or losses are covered by insurance or fall within the boundaries of acceptable risk.	Medium
	No action will be taken against individuals, or events involve low value assets.	Low
Provide information on actor activity over a period of time	Actor behavior is a concern to boards, customers, or regulatory entities, who require the organization to provide this information.	High
	Accountability is an organization concern and not a legal or external mandate, or activities and behavior patterns involve assets of medium value.	Medium
	Actions are not long-lasting and are of minimal impact.	Low
Be able to determine what captured information is relevant	Event information is to be used by boards, customers or regulatory entities who require the organization to provide this information.	High
	Accountability is an organization concern and not a legal or external mandate, or activities and behavior patterns involve assets of medium value.	Medium
	Only a small amount of audit log information is captured, or the overall need for audit service is low.	Low

Table 11.3 Audit service requirements factors (*continued*)

GENERIC REQUIREMENT	FACTOR	RESULTING PRIORITY
Perform its service when needed	The need for accountability is high, and security accounting is the only source of this information.	High
	The need for accountability is moderate, or alternative sources of accounting information are available.	Medium
Provide reliable and accurate information	The need for accountability is high, or security accounting information must be provided to an outside organization.	High
	The need for accountability is moderate, and only required inside the organization.	Medium

Table 11.4 Resolution of example problem for AUDIT REQUIREMENTS

REQUIREMENT	MUSEUM PRIORITY AND CONCERN
Provide information about malicious and unwanted events	HIGH – The museum decision makers want to audit all activity across the organization.
Provide information associating actors with events	HIGH – The museum decision makers want information that can hold people responsible for malicious activities.
Provide information on actor activity over a period of time	HIGH – The museum decision makers want information audited over a six-month period.
Be able to determine what captured information is relevant	MEDIUM – It is important for the museum to get as much factual data as possible. However, they would not expend a large amount of resources to do so.
Perform its service when needed	LOW – Although important to have audit ready when it is needed, the museum decision makers need audit every six months. They would not need to expend resources to make audit highly available.
Provide reliable and accurate information	HIGH – The integrity of data is critical to the museum obtaining an accurate report. The museum would allocate resources to ensure that the information they start with is in fact accurate.

customers over several decades. However, some publications on security audits and audit requirements exist:

- ISO standards [ISO13335-4] and [ISO17799] discuss security audits as one of the primary safeguards.
- [ISO15408] is an international standard that defines evaluation criteria for information technology security. It includes a class or family of criteria that address audit requirements, including data to be generated, analysis to be performed, and event storage.
- [COBRA02] discusses the COBRA method of security audit that includes questionnaires, checklists, and a tool to help automate audits.

Consequences

The following benefits may be expected from applying this pattern:

- It facilitates conscious selection of audit requirements, so that decisions about selecting audit mechanisms have a clear basis, rather than occurring in a vacuum.
- It promotes explicit analysis of trade-offs that encourages balancing and prioritizing of conflicting requirements and forces. This includes balancing the need for accountability with the need for privacy. This helps to avoid stronger than necessary audit mechanisms that would make it difficult for valid users, and at the same time it helps to avoid weaker than necessary audit that makes it easy for unauthorized actors to avoid.
- It results in documentation of audit requirements that communicates to all interested parties and is useful in determining the adequacy of accounting services such as audits.
- The explicit requirements resulting from the pattern foster a clear connection of requirements to audit policies. This also encourages organizations to make their accounting policies more explicit.

The following potential liabilities may arise from applying this pattern:

- It requires an investment of resources to apply the pattern, including time to analyze domains and audit needs. In some cases the cost of applying the pattern may exceed its benefits.
- It poses a danger of possible violation of privacy rights if extensive data is captured and analyzed. You can mitigate this by capturing and analyzing the minimum amount of data, and by working closely with your legal department.
- The formal selection process may be too long and costly and produce too much overhead. You can mitigate this in the same ways as noted above.

- Specific circumstances might not be covered by generic audit requirements. You can mitigate this by adding specific requirements and including them in the trade-offs.
- Documentation of requirements implies that they must be maintained as they change over time. You can mitigate this by keeping the requirements in a form that is easy to update, integrated with other system documentation.
- Perception of audit requirements can differ throughout an organization or in a particular domain. This may make it difficult to reach agreement on the relative priorities of requirements. On the other hand, bringing such disagreements to the surface may be a benefit of the pattern, because they can then be properly discussed and resolved.

See Also

After applying this solution, or in parallel, you can apply AUDIT TRAILS AND LOGGING REQUIREMENTS (378). This pattern captures the information used by AUDIT REQUIREMENTS (369).