11.3 Audit Trails and Logging Requirements

A service that captures security audit trails and audit logs must satisfy a set of requirements for both the service and the quality of service. The audit trails and logging function is to capture audit logs and audit trails about events and activities that occur within an organization or system, to enable reconstruction and analysis of those events and activities. While each situation that calls for an audit trail is unique, there are common generic requirements that apply to all audit trails and logging situations. This pattern provides a common generic set of audit trail requirements. The pattern also helps you to apply the general requirements to your specific situation, and helps you to determine the relative importance of conflicting requirements.

Example

The new museum wing for gemstones keeps its most precious gems in a room with limited access. The room's access is controlled by electronic badge access. Cleaning personnel, scientists and other authorized personnel need special badges to access the room. As an extra precaution, the museum would like a way to track access to the room by individuals and by roles. Samuel the museum system engineer needs to specify the requirements for audit trails and logging (AT&L) of activities related to this limited access room, and the relative importance of those requirements, as a means to drive and evaluate an AT&L service.

Context

Audit requirements and their relative importance are understood, for example, from applying AUDIT REQUIREMENTS (369). The planned uses of audit trails and logging are understood.

Problem

An organization needs to observe events and to revisit data related to those events to help achieve security properties in a system or domain, and to understand when and how security properties have been compromised. Audit trails and logging (AT&L) is a security service that automates the capturing of information about events and activities that occur within the organization. Audit trails are a series of records about system events or user activities. Audit trails can be used to reconstruct events, determine who is responsible for events, what malicious or unwanted activities have occurred,

and analysis of any problems. Logs are individual trails of information that may be combined into an audit trail.

You need a clear set of AT&L requirements to guide selection or implementation of an AT&L service and to determine if it is adequate to address organization or system needs. These requirements need to be prioritized to determine under what circumstances an organization should put more emphasis on one requirement over another.

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

The process of selecting and prioritizing AT&L requirements needs to balance the following forces:

- Capturing logs and audit trails increases the likelihood of achieving desired security properties, especially accountability
- Capturing logs and audit trails requires resources and entails cost
- Capturing logs and audit trails increases the risk of violating privacy laws, or of abusing such data, or of damaging the reputation of the collector
- A higher capacity of logs and audit trails enables greater volume and frequency of data acquisition, and a greater length of time for which data is available, which in turn supports increased accounting capability
- A higher capacity of logs and audit trails requires greater processing and storage resources
- Following accepted community AT&L requirements tends to save implementation cost, because tools are available to use
- Following accepted community requirements on collecting AT&L data may not give your organization exactly what you need
- AT&L data compression reduces required storage but requires compression and decompression tools

Solution

Specify a set of AT&L 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 performs the requirements process. An important first step is explicitly to define the domain for which you are specifying audit trails and logging requirements, such

as a specific system, or type of activities and events. You also define factors, such as organization constraints, that affect the specialization and importance of requirements. You then specify AT&L 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 following is a general set of requirements appropriate to an AT&L service.

- Acquire information about designated types of activities and events.

  An AT&L service must support the capture and storage of information related to security events that are potentially harmful or undesirable to the organization in audit trails or logs. This requirement is essential for stakeholders, who use the details provided to determine what the event was, when and where the event happened, and why and how the event happened. Significant related information should be stored along with the event information. For example, the time of day and date should be included in details of an event. Best practice does not require audit trails or logs to be provided for immediate viewing, although sometimes they are streamed to available workstations. Generally, audit trails and logs are subjected to audit analysis after the fact.

- Ensure that information acquired can help establish links between users and events.

  The AT&L service should ensure that the information acquired can be used to establish links between user activity and some event. The AT&L service needs to allow its users to acquire identifiers that represent the identity of a user uniquely and a description of their activities at the time the event was captured. This requirement is essential for accounting for user actions. Stakeholders use the provided details to determine who the actors are who engage in malicious or unwanted activity, and eventually assign the responsibility of the event to those actors.

- Ensure that information acquired is in a form that users can interpret.

  An AT&L service must not only capture information about events, but also ensure that the information is in a form that the user can understand. This requirement is essential for facilitating understanding of events and making informed decisions.

- Enable users to reconstruct events captured from disparate sources.

  Regardless of where or when parts of an event are captured, an audit trail creates a comprehensive view of the event. The audit trail may come from disparate sources, but collectively it forms a more complete view of the event. Users of the AT&L service should be able to acquire information as a single view

about events even though parts of the information are gathered from multiple sources. This requirement is essential for determining what an event was, performing investigations into malicious events, and piecing together information to determine event history.

- Enable users to repeatedly examine the information derived from an event.

  Scrutinizing events can help address future security breaches. Audit trails and logs gathered by this service need to be generally available for all accounting mechanisms and for extended periods of time, for potential event clarification or elaboration, as necessary. This requirement is essential to support users who need to revisit events to derive more information or re-examine conclusions drawn from earlier scrutiny.

- Perform its service when needed.

  An AT&L service needs to be able to provide its services during times where the tracking of events is absolutely important. During operation the AT&L service is processing information about events that could cause significant damage to the organization, and the AT&L service needs to be able to continue functioning during those high-impact events. This requirement is essential to support availability, and concerns the readiness of the AT&L service.

- Protect the information it captures.

  The AT&L service needs sufficient protection for its activity within the organization, and must afford a reasonable level of protection for the information being processed. The AT&L service should ensure that information intended for authorized users is not accessible to malicious actors. The AT&L service should also ensure that the information it provides to a user retains its accuracy. This information gives decision makers insight into how well the AT&L information is protected from malicious actors and how reliable the AT&L information is to use. This requirement is essential to support confidentiality, integrity, and privacy, and concerns the trustworthiness of the information the AT&L service provides.

- Provide accountability for changes to audit trails and logs.

  The AT&L service should provide information about an event that resulted in unauthorized or authorized access to information that the AT&L service provides. Event information needs to include all actor identifiers and events that occurred. This requirement is essential to support accountability.

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).

Implementation

This section first provides more detail on the process that was summarized in the Solution section, then discusses factors in determining the 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 AT&L service is needed.

   Ensure that the domain has been identified and scoped: typical AT&L domains include information system, physical facility, network, portal, 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 AT&L 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 uses of AT&L, AT&L needs, organization constraints, and priorities. You can find a general candidate set of factors below.
3. Specify AT&L requirements for the target AT&L domain.

   To do this, specialize the set of generic requirements given in the Solution section.
4. Define the relative importance of specific requirements.

   You can find more details about the association of factors and requirements below.

Factors in Determining Relative Importance

Table 11.5 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.

Table 11.5 Audit trail and logging service requirements factors

GENERIC REQUIREMENT	FACTOR	RESULTING PRIORITY
Acquire information about designated types of activities and 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
Ensure that the information acquired can help establish links between users and 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.	Medium
	No action will be taken against individuals, or events involve low value assets.	Low
Ensure that information acquired is in a form that users can interpret	Immediate response is needed to a critical event, and precise understanding is essential.	High
	Event responses allow for reasonable delay in reaction, or only general understanding is needed.	Medium
	Event responses are not time critical.	Low
Enable users to reconstruct events captured from disparate sources	Insurance or recoup of financial losses is critical.	High
	Organization is aware that it has events that span multiple areas.	Medium
	Events are localized or do not have multiple sources.	Low
Enable users repeatedly to examine the information derived from an event	Events and the information derived from event capture are critical to organization operations.	High

Table 11.5 Audit trail and logging service requirements factors (*continued*)

GENERIC REQUIREMENT	FACTOR	RESULTING PRIORITY
	Event information can be derived with a reasonable amount of scrutiny.	Medium
	Events are short-lived and simple.	Low
Perform its service when needed	Available AT&L is critical to event traceability.	High
	Losses due to unavailable AT&L are covered by insurance or fall within the boundaries of acceptable risk.	Medium
	No immediate need to respond to events.	Low
Protect the information it captures	Information found in audit trails is sensitive or information must be provided to an outside organization.	High
	Information is used only internally, or the information is not sensitive.	Medium
Provide accountability for changes to audit trails and logs	Legal mandate to provide that information, or needed for insurance purposes.	High
	Internal organization decision determines the consequences for the malicious actors.	Medium

Example Resolved

Samuel the museum systems engineer defines the museum rooms where precious gems are kept as an AT&L domain. Table 11.6 shows the museum concerns and associated requirements priorities Samuel has specified for this domain.

Known Uses

The general AT&L requirements and the process of specifying AT&L 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

Table 11.6 Problem example resolution for audit trails and logging requirements

REQUIREMENT	MUSEUM PRIORITY AND CONCERN
Acquire information about designated types of activities and events	HIGH – The museum decision makers want to enforce AT&L services for this domain across the organization.
Ensure that information acquired can help establish links between users and events.	HIGH – The museum decision makers want information from the AT&L service to be immediately usable to substantiate user involvement with events.
Ensure that information acquired is in a form that users can interpret	MEDIUM – Obviously, the museum would want the information to be as coherent as possible, but the priority is tracking of activities. The museum would be willing to trade off users taking a bit longer to understand information against having all information available to scrutinize.
Enable users to reconstruct events captured from disparate sources	LOW – In general this is an important requirement, but in this case the museum is interested in tracking the activity of access to the badge-protected room specifically, so logs from this room are most important.
Enable users repeatedly to examine the information derived from an event	MEDIUM – The ability to scrutinize the information facilitates the tracking of activities in the long term. This is useful but not critical for this domain.
Perform its service when needed	HIGH – The museum absolutely wants to have this ability to track activities for this domain even under emergency conditions. AT&L needs to be able to demonstrate that it can do this.
Protect the information it captures	HIGH – To have trust in the tracking information, AT&L needs to demonstrate that its information can be trusted.
Provide accountability for changes to audit trails and logs	MEDIUM – The museum wants to know who changes the information, but this is less important than acquiring and protecting the information.

multiple customers over several decades. However, some publications on security AT&L and AT&L requirements exist. Examples are:

- ISO standard [ISO13335-4] discusses AT&L 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 AT&L requirements, including event storage and audit trail availability.

Other more general discussions of AT&L practice are available in [Abrams95], [Bace01], [Cugini00], [DCD+02], [NIST800-12], and [Wheel99].

Consequences

The primary benefit is the existence of a set of explicit AT&L requirements for a given system or security domain. The relative importance of the requirements is identified. You may expect the following benefits from applying this pattern:

- It facilitates the conscious selection of AT&L requirements, so that decisions about selecting AT&L 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 AT&L mechanisms that would make it difficult for valid users, and at the same time it helps to avoid weaker than necessary AT&L that makes it easy for unauthorized actors to avoid.
- It results in documentation of AT&L requirements that communicates to all interested parties and is useful in comparing the adequacy of alternative implementations of AT&L services.
- The explicit requirements resulting from the pattern foster a clear connection of requirements to audit and logging 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 AT&L 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 AT&L 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 AT&L 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 then they can be properly discussed and resolved.