11.1 Security Accounting Requirements

A security accounting service must satisfy a set of requirements for both the service and the quality of service. The function of security accounting is to track security-related actions or events, such as damage to property, attempts at unauthorized database access, or transmission of a computer virus, and provide information about those actions. While each situation that calls for security accounting is unique, there are common generic requirements that apply to all security accounting situations. This pattern provides a common generic set of security accounting requirements. The pattern also helps you apply the general requirements to your specific situation, and helps you to determine the relative importance of conflicting requirements.

Example

Gemstones within a museum are objects used in archeological research. They are also cleaned, transported and handled by several authorized personnel. The museum is interested in protecting museum assets from theft, damage or any mishandling. The museum is serious about assigning responsibility for any asset compromise or attempts to compromise assets. The museum needs to identify the requirements for the key components of a security accounting service that will help them protect their valuable gems and help assign responsibility for attempts to compromise their assets.

Based on the results of applying ENTERPRISE SECURITY SERVICES (161), Samuel the museum system engineer understands that the museum needs accountability of actions and events when the gems are transported or handled, and accountability of actions on the information about the gems, which is stored in a database. The museum needs to be able to assign responsibility for any asset compromise or attempts to compromise assets. For example, the museum needs to know who is responsible for transporting a gem. When information about a gem, such as its current location or its recorded carat weight, is entered or modified, the museum needs to know who made the addition or change. But Samuel also understands that the need to track and account for these actions and events must be balanced with the need for privacy and ease of operations. Therefore, Samuel needs to specify a balanced set of requirements for security accounting and the relative importance of those requirements, as a means of driving and evaluating an appropriate security accounting service for the museum. How can Samuel define such a set of requirements?

Context

The planned uses of security accounting are understood, for example, from applying ENTERPRISE SECURITY SERVICES (161). Asset types with a need for security accounting

services are known, and the general types of actors that are to be held accountable are known. Actor types can include humans, software, business or automated processes, or information systems. Actors can be internal to an organization, such as an employee, or external, such as a supplier or customer. Asset types include both physical and information assets. The degree of confidence needed for the security accounting services by general asset types is known in relative terms. For example, a museum needs a very high degree of confidence in knowing who broke into the museum and stole a valuable gem, but it needs a lower degree of confidence in knowing who defaced the outside of the museum building.

Problem

Security accounting is an activity that takes in the detectable data from an event and provides some security-relevant information about that event to a human. A basic accounting sequence is completed when security-relevant information associated with an event of interest is provided to the accounting user. You need a clear set of requirements to ensure that the strategy employed for a security accounting system actually satisfies the needs of the organization or system. Requirements for security accounting often conflict with each other, and trade-offs between them are often necessary. You need to prioritize these requirements to determine under what circumstances you should put more emphasis on one requirement over another.

How can you determine specific requirements for a security accounting service, and their relative importance?

Below are examples of different security accounting use situations that define different security accounting needs for an organization. Many other security accounting service use scenarios are possible.

1. Security accounting is used to establish how well financial assets are being protected over a five-year period. The organization suspects that authorized access to the records is being used to misdirect funds, so security accounting is employed to help identify any perpetrators.
2. Security accounting is used to search for any intrusions into the organization's network. Security accounting monitors network traffic and compares that information to authorized traffic. Security accounting issues an alert if there is activity that is unwanted or unexpected.
3. Security accounting is used to establish a documented trail of evidence for global, very large, financial transactions. Security accounting must capture transaction terms, and the identities of parties that engage in such transactions. The terms and party identities must be accessible for review and reported to decision makers. There is a risk of large financial loss, and therefore the security accounting service must be as accurate as possible.

The process of selecting and prioritizing accounting requirements needs to balance the following forces:

- You can use security accounting to help achieve desired security properties, especially accountability
- Applying accounting has many associated costs (support personnel, software, additional processing time, and so on) that are counter to the organization goal of minimizing total costs
- Collecting extensive relevant raw accounting data increases the likelihood of achieving accountability
- Collecting extensive raw accounting data increases the risk of violating privacy laws, or of abusing such data, or of damaging the reputation of the collector
- The range of time in which accounting may be needed for an event is very broad, ranging from near-real-time to years after the event
- Types of events for which accounting is needed may include repeatable, consistent events, as well as ad-hoc events
- Applying accounting adds complexity to the administration processes, which is counter to the organization goal of minimizing and simplifying administrative and maintenance processes
- Accounting needs to interface with other security services (for example, access control, I&A), thereby increasing the complexity of the software, which is counter to the organization engineering goal to maximize service independence
- Supporting multiple types of accounting policies across an organization increases complexity, which is counter to reducing overall costs
- The elements of the security accounting service need protection if the service is to perform its function

Solution

Specify a set of accounting 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 security accounting requirements, such as a specific system or facility. You also define factors that affect specialization and importance of requirements, such as organization constraints. Then you specify security accounting

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

Security accounting is a security service that involves the capturing, storage, reviewing and reporting of security-relevant information from an event. The following is a general set of requirements appropriate to security accounting services.

- Provide information about specific events.

  A security accounting service must allow information to be obtained about events that are undesirable or harmful to the organization. The time of day, day, month and year are all pieces of information that should be included in details of an event. The details provided by security accounting can either be given as they are captured or made available for scrutiny at a later date. This information will be used to help protect assets by allowing an accounting user to determine what the event was, who was involved, when and where the event happened, why and how the event happened, and how an asset was affected by an event. It also allows actions to be taken to preserve the confidentiality, integrity and availability of an asset based on the type of event.
- Provide information about who engages in activities.

  This requirement is essential for accounting for user actions. The security accounting service should allow information to be obtained that can be used to establish links between user activity and some event. Security accounting needs to allow its users to determine who the actors are who engage in a malicious or undesired event, and a description of their activities at the time the event was captured. This information will be used to help assign responsibility to an actor for the event and its consequences.
- Provide a degree of confidence that its service will function when needed.

  This requirement is essential to support security availability. Security accounting needs to be able to provide its services during times when the tracking of events is absolutely important. During operation the security accounting service should be aware of events that could cause significant damage to the organization, and it needs to be able to continue functioning during those high-impact events. Whether the information needed from security accounting is in real-time or non-real time, security accounting is required to be ready to perform its function.
- Provide a degree of confidence that the information it provides is accurate.

  This requirement is essential to support integrity. Security accounting should provide information about the accuracy of the data it provides to a user. This information gives decision makers insight into the trustworthiness of the security accounting information.

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 access control-specific requirements identified and discussed above.

Implementation

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

Process Guidelines

The requirements process typically includes these steps:

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

   Ensure that the domain has been identified and scoped. Typical security accounting domains include information system, physical facility, network, portal, or entire organization. The domain consists of at least three parts: a defined scope of actors, a defined scope of assets, and a defined scope or set of events that involve actions on those assets. Note that other terms are also used in place of actor, asset, action. For example, [ISO15408] uses subject, object, and operation, respectively. Other constraints may also bound the domain—for example, the accounting requirements for real-time service may differ from those for multi-year service. These might represent two distinct domains.
2. Specify a set of factors that affect the specialization and importance of requirements.

   The factors include uses of accounting, accounting needs, organization constraints, and priorities. You can find a general candidate set of factors below.
3. Specify accounting requirements for the target accounting domain.

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

Requirement Priority Factors and Impacts

Table 11.1 reiterates the generic requirements described in the Solution section, along with factors for judging their relative importance to the organization. For each

requirement, positive and negative impacts of the factors on importance or priority of the requirement are also provided.

Table 11.1 Accounting service requirements importance factors

GENERIC REQUIREMENT	FACTOR	RESULTING PRIORITY
Provide information about events (what, when, where, why and how)	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 about who engages in activities (who)	Assigning responsibility is a 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 a degree of confidence that the service will function 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 a degree of confidence that the information the service provides is accurate	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

Example Resolved

Samuel the museum systems engineer defines several domains, because the importance of accounting requirements varies for different asset types. The domains include high value gemstones, the database system that records information about gems, and the physical facilities that house the gem exhibits. Table 11.2 shows the requirements ratings Samuel has specified for the high-value gems domain. Not surprisingly, all security accounting requirements are rated High for this domain.

Known Uses

The general accounting requirements and the process of specifying accounting requirements described in this pattern are widely known, but are generally used informally, as opposed to being codified or published. The requirements as stated here represent a consolidation of MITRE Corporation's experience in working with multiple customers over several decades. However, some publications on accounting requirements also exist.

For example, the Common Criteria [ISO15408] is an international standard that defines evaluation criteria for information technology security. It includes some discussion of accounting requirements, especially in the context of the potential conflict between accounting and privacy, or in some cases between accounting and availability. An example of the latter is specifying the required action when an audit trail is full: should you make the associated asset unavailable, or should you retain availability of the asset and allow collection of accounting data to lapse?

Table 11.2 Museum requirements for security accounting service

REQUIREMENT	MUSEUM REQUIREMENT RATING
Provide information about events (what, when, where, why and how)	HIGH – The museum decision makers want to track all activities and events regarding high value gems across the organization.
Provide information about who engages in activities (who)	HIGH – The museum decision makers want information that can hold people responsible for malicious activities regarding high value gemstones.
Provide a degree of confidence that its service will function when needed	HIGH – The museum would like to have a high level of certainty that accounting will perform its function, and specifically requires a 0.9999 availability rating.
Provide a degree of confidence that the information it provides is accurate	HIGH – The museum would like to have certainty that it can rely on the information that security accounting provides.

Consequences

The following benefits may be expected from applying this pattern:

- It facilitates conscious selection of security accounting requirements, so that decisions about selecting security accounting 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 security accounting mechanisms that would make it difficult for valid users, and at the same time it helps to avoid weaker than necessary security accounting that makes it easy for unauthorized actors to avoid.
- It results in documentation of security accounting requirements which 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 security accounting 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 security accounting needs. In some cases the cost of applying the pattern may exceed its benefits.
- It poses a danger of over-engineering and complexity creep if stakeholders are offered too many options. You can mitigate this by using the requirements only as guidelines for analysis, or by selecting parts of the pattern that give the most help.
- 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 security accounting 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 security accounting 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.

See Also

After applying this pattern, the next step typically is to apply AUDIT REQUIREMENTS (369), AUDIT TRAILS AND LOGGING REQUIREMENTS (378), INTRUSION DETECTION REQUIREMENTS (388), or NON-REPUDIATION REQUIREMENTS (396).