9.1 Access Control Requirements

The function of the access control security service is to permit or deny someone the right to perform an action on an asset, such as create, read, modify, or delete a data file. While each situation that calls for access control is unique, there are common generic requirements that apply to all access-control situations. This pattern provides a common generic set of access control requirements. The requirements address both the access control function and the properties of the access control service, such as ease of use and flexibility. 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

A new wing of an existing museum of gemstones is to be opened. The wing will house gems of varying value, some of which are owned by the museum and some of which are on loan. Some of the gems are famous stones whose loss would involve much media publicity. The wing will house valuable gems on display, low-value gems in a hands-on exhibit, and gems of all values in working areas of the wing that are not open to the public.

Based on the results of applying ENTERPRISE SECURITY SERVICES (161), Samuel the museum's system engineer understands that the museum needs to control access to the gems and to the information related to gems. An obvious example is that an attempted access by Theo the thief to steal a gem should be denied. Another example is that the recorded carat weight for gems should not be modifiable by unauthorized people. An unauthorized change in recorded carat weight could change a gem's value, change insurance costs, or even signal the beginning of an attempt to carve off a piece of the stone.

But Samuel also understands that the need to deny unauthorized access must be balanced against the need to permit authorized access. For example, the best safeguard against theft of a gem is to lock it up in a vault and not tell anyone where it is. But this would interfere with a primary goal of the museum, which is to display gems for public viewing. Therefore, Samuel needs to specify a balanced set of requirements for access control and the relative importance of those requirements, as a means of driving and evaluating an appropriate access control service for the museum. How can Samuel define such a set of requirements?

Context

An organization understands how it plans to use access control, for example, from applying ENTERPRISE SECURITY SERVICES (161). An organization understands the general types of actors, assets and actions that are to be subject to access control. An access control rule permits an actor to perform an action on an asset—for example, user A is granted permission to modify file F. 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. Action types include both physical and automated actions. Common actions include create, see, use, change, and destroy or delete. Asset types include both physical and informational assets.

Problem

You need a clear set of requirements to ensure that the strategy employed for access control actually satisfies the needs of the organization or system. Requirements for access control often conflict with each other, and trade-offs among them are often necessary. The conflict stated in the example is that the need to protect gems by denying unauthorized access must be balanced with the need to permit visitors to view the gems.

How can you determine the specific requirements for an access control service, and their relative importance?

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

- You can use access control to help achieve desired security properties, especially confidentiality and integrity.
- Access control has many associated costs, not only the money for its deployment, but also support personnel, software, latency, annoyance for users, and so on.
- Access control adds complexity for software, systems, users and administration.
- Access control should be consistent with the organization's security policies, and specifically with access control policies.
- The complexity of administering access control must be reasonable or the administrator will make errors, resulting in vulnerabilities.
- You cannot deploy access control as a stand-alone facility, it needs to interface or integrate with other security services, thus increasing complexity.
- Extremely high levels of control tend to achieve the desired result of denying most unauthorized access, but also tend to achieve the undesired result of denying more authorized access and making the asset or system harder to use.

- Moderate levels of control tend to achieve the desired result of allowing most authorized access, but also tend to achieve the undesired result of allowing more unauthorized access.
- The elements of the access control service need protection if the service is to perform its function.

Solution

Specify a set of access control 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 requirements capture. An important first step is explicitly to define the domain for which you are specifying access control requirements, such as a specific system or facility. You also define factors that affect specialization and importance of requirements, such as organization constraints. You then specify access control 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 Access Control Requirements

The following is a general set of requirements appropriate to access control services. An engineer will need to consider each of these and determine its priority based on criteria specific to the target domain, as well as on broader organization constraints. Additional requirements may be added to this list to address the system's unique characteristics. Some of the general requirements below represent access control functional requirements. The remaining requirements represent access control non-functional requirements, including requirements for security of the access control service.

- Deny unauthorized access

  One primary purpose of access control is to deny unauthorized access requests. No access control service is perfect, and therefore errors will be made in which unauthorized access will be permitted. The goal of this requirement is to keep such errors to a minimum. The importance of this requirement needs to be weighed against requirements for other functional services.

- Permit authorized access

  The second primary purpose of access control is to permit authorized access requests. The goal of this requirement is to keep to a minimum errors in which authorized access will be denied. Sometimes this type of error is caused by an

operational error in the access control service; sometimes it is caused by the service's inability to support a desired authorizations policy, and sometimes it is caused by an incorrect access control service policy statement.

- Limit the damage when unauthorized access is permitted

  A strong security principle is to avoid relying on a single point of failure. This requirement says that a single error in which unauthorized access is permitted should not permit access to multiple actions. The well-known defence-in-depth approach, using multiple layers of security, could be used in addressing this requirement. This requirement needs to be weighed against the 'limit the blockage' and 'minimize burden' requirements below.

- Limit the blockage when authorized access is denied

  Consider an access control error in which authorized access is denied. This requirement says that a single failure of this type should not cause a serious interruption of business by denying many actions. This requirement needs to be weighed against the 'limit the damage' requirement above and the 'minimize burden' requirement below.

- Minimize the burden of access control

  The burden of access control is an issue that affects multiple players and activities, including system users, interaction with other security services, processing resources, and implementers of the access control service. Each of these will be discussed briefly.

  The access control service should control similar actions in a similar way, to minimize the perceived complexity for human users and developers of non-human actors, and to minimize the likelihood of errors. The access control service functionality depends on effective I&A. I&A should therefore have an interface that accommodates the access control service easily.

  Processing overheads can cause reduction in availability of operations on assets for authorized users. This reduction may be due to blocking requests that should be permitted, or due to interruptions of the request flow caused by the access control service. Latency can become a factor. For example, when every action needs to request permission from a remote access control server, overhead can be significant.

  Factoring the commonalities among access control requirements to produce a small generic set, as in this pattern, has several purposes. One of them is to reduce the burden on access control implementers by enabling them to define the system with a minimal set of primitives.

- Support desired authorization policies

  The function of the access control service is to enforce the authorization policies defined to meet the business needs for the system or domain for which the

service has responsibility. The access control service should be designed to enforce the required policies.

Definition and selection of access control policies is a key element. In fact, access control is about defining policies for authorization and then enforcing these policies through specific mechanisms. For example, a fundamental policy is 'open versus closed' systems. In an open system everything is allowed unless explicitly forbidden. In a closed system everything is forbidden unless explicitly allowed. Another set of fundamental policies is defined by the choices among the access control models discussed in Chapter 8: access matrix, role-based access control, multi-level control, and attribute-based control. Any access control system must implement one or more of these.

At the most generic level, therefore, the requirement is that an access control service must support all desired authorization policies. At a more specific level, authorization policies are selected that the implementation must enforce.

- Make the access control service flexible

  Authorization policy statements sometimes change. This requirement says that adaptation to those changes should be fast, easy, and reliable. That is, the access control service should accommodate policy changes without high cost, complex administration, or increased difficulty of validating that the access control service requirements accurately reflect the authorization policy statements.

  Access control also needs to be flexible, to accommodate legitimate operational changes or exceptions. For example, when the threat of terrorist attack is perceived to be high the organization may require stringent checks at facility entry points at the cost of substantial delays. Employees and customers may tolerate such delays for a week or two, but not for months. An opposite example is the case of a hospital, where, if a patient's life is at stake, blocking access to normally-protected patient data may be wholly unacceptable. The system should make some provision that allows access, such as emergency override. At the same time, to provide protection in such incidents, the access control service should record the emergency activity automatically. This will enable a forensic activity or an audit to determine the facts about the violation of normal access rules, and to determine their legitimacy.

  Another area of flexibility is granularity. An access control service must be able to support a policy that supports both fine-grained control, such as specific elements in a database, or coarse-grained control, such as a whole database or group of users. In addition, an access control service should be able to support conditional authorization, such as permitting access at certain times of the day but not at others.

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 need to be considered in each requirements pattern. The requirements are: minimize time and effort to use, mismatch with users, risks to user safety, costs of per-user setup, costs of maintenance, management, and overhead, and changes needed to existing system infrastructure. The final requirement is to provide security protection of the service and its assets. Further discussion of each of these cross-cutting requirements, including implementation factors, is given in I&A REQUIREMENTS (192).

Implementation

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

Process Guidelines

The requirements process typically includes these steps:

1. Establish the domain for which the access control service is needed.

   Ensure that the domain has been identified and scoped. Typical access control domains include information system, physical facility, network, portal, or entire organization. Typical scope definition includes a defined set of actors, of assets, and of actions on those assets. Other constraints may bound the domain—for example, the access control requirements for entering a designated facility during normal work hours may differ from the requirements during out of work hours such as night-time and weekends: these would represent two domains.

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

   The factors include uses of access control, access control needs, organization constraints, and priorities. You can find a general candidate set of factors in the next section.

3. Select one or more appropriate access control policies, such as a closed system policy and a role-based model, as discussed above.

   For security sensitive areas, it is generally considered better practice to follow a closed system policy, that is, to default to denial of access when it is not explicitly permitted. In less sensitive situations, an open system policy may be more appropriate, in which anything is permitted unless it is explicitly denied—for example, most information on public Web pages.

4. Specify the granularity levels at which access control will be applied.

   The level of granularity of the domain or asset to which access is specified can vary. For example, access to a physical facility such as a campus may be defined at the level of the entire facility, or a specific building, or a floor in the building, or a specific room. Access to a relational database may be defined at the level of the entire database, or to a specific partition or region, or a specific table, or specific rows in the table, or specific fields. The requirements need to specify the desired granularity, and often the requirement is to support multiple levels simultaneously.

5. Specify access control requirements for the target access control domain.

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

6. Define the relative importance of specific requirements.

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

Factors in Determining Relative Importance

Table 9.1 presents factors for judging the relative importance to the organization of the generic access control requirements that were identified in the Solution section. For each requirement, the table also describes how the factors affect the relative priority of the requirement. For an example of applying these factors to each requirement, see the Example section below.

Table 9.1 Access control requirements factors

GENERIC REQUIREMENT	FACTOR	IMPACT ON PRIORITY
Deny unauthorized access	When sensitivity of assets is very high, or ability to validate credentials of an actor is suspect, the preferred approach is to block all suspected unauthorized requests.	This requirement should have increased priority if allowing unauthorized access could cause significant damage to the system. This requirement needs to be balanced with the need to permit authorized access for business needs.
Permit authorized access	Users are a higher priority than assets and blocking authorized activities would create severe problems for the organization or system.	This requirement should have increased priority if denying authorized access would cause excessive levels of disruption of business functions, or excessive levels of user dissatisfaction with system. This requirement needs to be balanced with the need to deny unauthorized access.

Table 9.1 Access control requirements factors (*continued*)

GENERIC REQUIREMENT	FACTOR	IMPACT ON PRIORITY
Limit the damage when unauthorized access is permitted	Can use multiple levels of protection by increasing the number of actions required to achieve complete access.	This requirement should have increased priority if failure to block unauthorized access is likely to cascade into additional failures of security services. This requirement needs to be balanced with the need for ease of use: users may become frustrated with any multiple control paths they must navigate to gain access.
Limit the blockage when authorized access is denied	Consider high priority for this if user accessibility is of high importance.	This requirement should have increased priority if the controls are likely to cascade into excessive frustration and productivity loss of legitimate users due to erroneous denial of access. This requirement needs to be balanced with the need to deny unauthorized access.
Minimize burden of access control	System has tight constraints for performance and asset availability, as well as functionality of other services in the system	This requirement should have increased priority if a high burden of using the access control service would cause excessive levels of user dissatisfaction with system, or would disrupt business functions. This requirement needs to be balanced with the need to deny unauthorized access
Support desired authorization policies	The access control service is useful only if it supports the designated policies.	This requirement should always have high priority.
Make access control service flexible	Some organizations or domains have a diverse set of authorization policies, or the policies or access context change often, or policies need to operate in two or more modes, such as normal, increased security, and emergency override.	This requirement should have increased priority if your organization or domain has the characteristics described in this factor. Flexibility is important to permit users needed access in emergency situations, or to increase system protection when specific threats increase significantly. This requirement needs to be balanced with the need for ease of use and simplicity of design.

Example Resolved

Samuel the museum's system engineer defines the domain for access control to include the gem assets themselves, as well as sensitive information about the gems. Although these may be regarded as two different domains for some purposes, Samuel decided to define a single requirements set for both. A clear starting point is a closed authorization policy, in which access to both the gems and information about the gems is forbidden unless explicitly allowed.

Samuel, in consultation with Edward the museum architect, has also determined that the access control service will give greater importance to protection of the assets and sensitive asset information than to immediate satisfaction of user requests. The museum is inclined to disallow even valid requests if anything suspicious is detected in the activity. On the other hand, they will strive to make their unsophisticated user base less aware of the security controls by not presenting multiple rechecking at every step. The actual system policy approaches are known, and Samuel does not anticipate any need for expansion of the number or type of policies enforced. Samuel sees two potential modes of operation: normal conditions and an emergency lock-down.

Table 9.2 shows the requirements Samuel specified for the stated domain.

Known Uses

The general access control requirements and the process of specifying access control 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 experience in working with multiple customers over several decades. However, some publications on access control requirements exist. The examples that follow emphasize the value of defining access control requirements explicitly, and the separation of policy from mechanism while maintaining adherence of mechanism to policy, consistent with this pattern.

- [LDAP00] is a discussion of access control requirements for LDAP. In addition to LDAP access control requirements, it discusses policy requirements, granularity, and nonfunctional requirements, especially usability.
- [Coe03] discusses access control requirements in the context of virtual organizations. The authors discuss authorization and access control-related languages and standards, and access control policy requirements. They stress the importance of defining security domains for access control, and interoperability and composition among domains and their associated policies and models.
- [Eve04] is a case study used to motivate access control requirements. It discusses granularity and some of the nonfunctional requirements identified in this pattern.

Table 9.2 Museum requirements for access control service

GENERIC REQUIREMENT	MUSEUM REQUIREMENT AND PRIORITY
Deny unauthorized access	High priority – the museum requires access control to provide a certainty of at least 0.9999 for denying unauthorized access to high-value gems, meaning that the service shall allow no more than one successful access out of 10,000 unauthorized attempts. The museum requires that access control provide a certainty of at least 0.999 for denying access to the associated gems information.
Permit authorized access	Moderate priority – the museum regards user convenience as a lower priority than protecting the assets under its care. The museum requires access control to provide a certainty of at least 0.98 for permitting authorized access to gems or gem information, meaning that the service shall deny no more than one access out of 50 authorized requests for access.
Limit the damage when unauthorized access is permitted	High priority for gems – the museum places high priority on avoiding inadvertent access to all gems. If Theo the thief is successful at circumventing access control to get his hands on one gem, that success must not give him access to all the other gems. Moderate priority for gem information – the priority of this requirement for gem information is balanced by the need for access by gem researchers, with the assumption that the user base of researchers will not be overly knowledgeable with regard to the information system.
Limit the blockage when authorized access is denied	Low priority – the museum gives higher priority to asset protection than to user access. They would prefer to occasionally have to address a locked out user rather than lose an asset, or sensitive information about that asset.
Minimize burden of access control	Moderate priority – the museum will try to attain a middle ground with this requirement. They want effective access controls, but they don't want to impact other functional services, create bottlenecks, or create denial of service scenarios.
Support desired authorization policies	High priority – the museum has defined a closed system access control policy that focuses on the gems they protect and associated information. Samuel does not see that scenario changing over the long term.
Make access control service flexible	Moderate priority – the museum requires the access controls to change when they need to operate in emergency lock-down mode, as opposed to normal operating conditions, but the policy is not expected to change significantly.

- [ISO15408] is an international standard that defines evaluation criteria for information technology security. It includes a class or family of criteria that address the requirements for functions to define authorization or access control policy, and explicitly authorize or deny access of a subject to perform an operation on an object in conformance with that policy.
- [Vim03] identifies general desiderata or requirements for access control, and how they are expressed in policies. It discusses how the requirements are addressed in several current operating systems, database management systems, and network solutions.

Consequences

The following benefits may be expected from applying this pattern:

- It facilitates conscious selection of access control requirements, so that decisions about selecting access control 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. It helps avoid stronger than necessary access control that makes it difficult for valid users, and at the same time it helps avoid weaker than necessary access control that makes it easy for unauthorized actors to defeat.
- It results in documentation of access control requirements that communicates to all interested parties and also provides information for security audits.
- The pattern fosters a clear connection of requirements to authorization policies: this also encourages organizations to make their policies more explicit.

The following potential liabilities may arise from applying this pattern:

- An investment of resources is required to apply the pattern, including time to analyze domains and access control 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 as guidelines only for analysis, or by selecting parts of the pattern that give the most benefit.
- The formal selection process may be too long and costly and produce too much overhead. You can mitigate this in the same way as noted above.
- Specific circumstances might not be covered by generic access control 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 access control requirements can differ throughout an organization or in a particular domain. This may make it difficult to reach agreement on 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 solution, the next step typically is to apply architecture or design patterns that help satisfy the specified requirements for access control.

Patterns presented in this chapter include the following: SINGLE ACCESS POINT (279), CHECK POINT (287), and SECURITY SESSION (297) build on each other, showing how to implement an architecture providing I&A and access control to an application or system. The remaining two patterns, FULL ACCESS WITH ERRORS (305) and LIMITED ACCESS (312), demonstrate two opposite strategies for dealing with the problem of how to present a secured system to its users in which different users will have different access rights.