7.1 I&A Requirements

An identification and authentication (I&A) service must satisfy a set of requirements for both the service and the quality of service. The function of I&A is to recognize an individual and validate the individual's identity. While each situation that calls for I&A is unique, there are common generic requirements that apply to all I&A situations. This pattern provides a common generic set of I&A 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 museum gemstones wing will build on the parent museum's intranet, with workstations distributed throughout multiple departments. Based on applying ENTERPRISE SECURITY SERVICES (161), the museum recognizes the need for specific security functions. Among these are access control and security accounting. Both of these functions rely on an I&A service to establish identity. What kind of I&A service does the museum need to support these functions? What other situations call for an I&A service in the museum? After some analysis, Samuel, the museum's system engineer, and Edward, the enterprise architect, come up with these possible situations that require I&A services:

- Establishing physical access to the museum during business hours
- Establishing physical access to the museum by staff during outside business hours
- On-line access to the intranet from within the local area network of the museum wing
- Remote on-line access to the museum's intranet
- Access to highly sensitive museum physical assets, especially gemstones
- On-line access to highly sensitive museum information assets
- Tracking who is downloading information from the publicly-available museum Web site
- Support non-repudiation of business transactions on the part of customers or partners
- Employee accountability of computer and network resource use within the museum
- Accountability to support identification of the source of computer viruses or a network denial of service attack

The engineers feel that these situations differ in their I&A requirements, but are not sure how to capture the differences. For example, a single mechanism for Web site I&A doesn't work, because Vic the visitor, downloading publicly-available information, has I&A requirements that differ from Manuela the museum manager, who is working from home and retrieving sensitive accounting data. Furthermore, for each of these situations, the museum wants to properly balance conflicting objectives, such as a service that detects would-be hackers versus a service that is easy for employees to use. Typically a strong I&A mechanism that detects most imposters, that is, people who falsely claim to be legitimate, are hard to use, while I&A mechanisms that are easy to use tend to give weaker protection, in too many cases concluding that an imposter is legitimate.

Samuel's initial thinking had been that he could simply select some I&A mechanism such as a password-based log-on or an employee badge. This has given way to the realization that more thought and consideration is needed to ensure that multiple I&A needs are properly addressed. Samuel and Edward recognize that they need to specify a clear and balanced set of requirements for each situation the requires I&A. How can they accomplish this?

Context

An organization or project understands its planned uses of I&A, for example, from applying ENTERPRISE SECURITY SERVICES (161), or from applying one or more of the pattern systems that use I&A, such as the patterns for access control in Chapter 8, 9 and 10 and the accounting patterns in Chapter 11.

The scope is known to be situations in which both identification and authentication are needed. Other situations exist in which only identification is needed without authentication, but those situations are not addressed in this pattern.

Problem

Requirements for I&A often conflict with each other, and trade-offs among them are often necessary. The conflict stated in the Example section is that strength of protection with I&A tends to conflict with ease of use.

I&A comprises both associating an identifier with an actor (identification) and verifying that the association is correct (authentication). I&A is a security service whose results are often used by other security services, including access control and accounting. A basic set of generic I&A requirements exists for all types of use and circumstances. However, these generic requirements need to be specialized for a given I&A domain. In addition, the relative importance of the requirements will vary based on the circumstances. What is needed is (1) to capture the specific set of requirements, and (2) to understand how to differentiate the relative importance of the requirements in specific circumstances to balance or resolve the conflicts.

How can you determine specific requirements for an I&A service, and their relative importance?

Determination of I&A requirements needs to resolve the following forces:

- Owners of I&A services want the services to perform their expected function, that is, correctly to determine whether an actor is associated with an identifier
- Incorrectly confirming the false claim of an imposter can lead to extensive disclosure of or damage to assets
- Incorrectly denying the true claim of a legitimate actor can lead to loss of productivity through denial of service or denial of access to authorized assets
- Users want I&A services to offer good quality of service: rapid response, proper functioning, easy to understand, safe, appropriate for category of user, and supportive of handicapped users
- The enterprise wants its I&A services to be cost effective and provide a good return on investment
- There are often reasons for making identifiers public—for example, e-mail identifiers need to be known so that others can send e-mail
- The I&A service will need to protect against the potential for stolen identities and the impacts of stolen identities and authenticators

Solution

Specify a set of I&A requirements for a specific I&A domain, 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 I&A requirements, such as a specific system or facility. Factors such as enterprise constraints that affect specialization and importance of requirements also need to be defined. The I&A requirements for the target I&A domain are then specified, using the generic requirements provided below. The final activity is to define the relative importance of the specified requirements.

Generic Requirements Description

The following set of generic requirements responds to the problem and forces described above. The first two represent I&A functional requirements. The remaining requirements represent I&A non-functional requirements, including requirements for security of the I&A service.

The following analysis is presented to help you understand and apply the first two generic requirements. For the I&A service properly to execute its function, it must be able to deny the identity claims of imposters, and confirm the claims of legitimate actors. In any given I&A episode, any of four outcomes is possible, illustrated in Table 7.1.

Table 7.1 Outcome of I&A situations

ACTUAL SITUATION	I&A SERVICE CONCLUSION	
	Confirmation of actor claim (You are Actor A)	Denial of actor claim (You are not Actor A)
Actor A claims to be Actor A	True positive	False negative
Actor B claims to be Actor A	False positive	True negative

The table shows that the four outcomes result from two variables, namely, the actual situation and the I&A service conclusion. One function of the I&A service is to confirm the identity of legitimate actors, that is, actors who are who they claim to be. This result is a true positive or true acceptance. The second function of the I&A service is to deny the identity of imposters, that is, actors who are not who they claim to be. This result is a true negative or true rejection. A perfect I&A service would result in 100% true positives in situations where the actor is legitimate, and 100% true negatives in situations where the actor is an impostor. But no I&A service is perfect, and two types of errors are possible. One type of error, called a 'false positive' or 'false acceptance,' is confirmation that an imposter is who he claims to be. In Table 7.1, the false positive is erroneous confirmation that Actor B is Actor A. The second type of error, called a false negative or false rejection, is denial that an actor is who he claims to be. In Table 7.1, the false negative is erroneous denial that Actor A is Actor A. If an error occurs, it is then propagated to the function that relies on the I&A service. For example, an access-control service may use a false positive from the I&A service to permit an imposter access to sensitive assets, which can then be damaged or destroyed.

The generic requirements are as follows.

Accurately Detect Imposters

In the context of Table 7.1, this requirement addresses the imposter situation, that is, Actor B claims to be Actor A. The requirement says that the I&A service must recognize that this actor is not Actor A, and deny the claim. The service must result in a true negative and not make the false positive error. Note that this requirement does

not ask the I&A service to recognize Actor B as Actor B, but only to recognize that this actor is not the claimed Actor A.

Accurately Recognize Legitimate Actors

In the context of Table 7.1, this requirement addresses the legitimate actor situation, that is, Actor A claims to be Actor A. The requirement says that the I&A service must recognize that this actor is Actor A, and confirm the claim. The service must result in a true positive and not make the false negative error.

A trade-off exists between this requirement and the previous one. A stringent I&A service that provides a very high probability of detecting imposters also tends to have a higher probability of denying the claims of legitimate actors. Conversely, a more accommodating I&A service that provides a very high probability of confirming legitimate actors also tends to have a higher probability of confirming the claims of impostors. When you apply this pattern to your specific system or organization, you need to determine which type of error is more important to avoid.

Minimize Mismatch with user Characteristics

An I&A service is typically used by different categories of users, such as level of experience. Both inexperienced users or novices, and experienced or sophisticated users, want the I&A services to interact with them at their own level. Some I&A techniques require more sophistication than others. Additional characteristics to be considered include fixed versus mobile location of users, and remote versus local users.

Minimize Time and Effort to Use

Performing I&A almost always costs users some time and effort in the process of acquiring access to an enterprise asset. For example, remembering and typing a password, or standing in line to be approved by a security guard, or assigning and maintaining certificates associated with a software module, is not as easy as not typing the password, not needing to wait for the guard, or not assigning the certificate. User effort and time delays associated with I&A adds to the bottom-line cost of enterprise operations, so that in general it is desirable to minimize the effort and time involved in performing I&A. Single sign-on (SSO) is one common approach to minimizing time and effort in the context of an enterprise network, by means of a single authentication that is performed when users initially access the network. This requirement is often in conflict with accuracy requirements, however.

Minimize Risks to User Safety

Issues of safety, such as requiring use of iris-scanning if users could be wearing gas masks, or damage done by retinal scanning, can preclude use of an authentication technique. This requirement is sometimes in conflict with accuracy requirements.

Minimize Costs of Per-user Setup

Establishing a new user or actor in an I&A domain involves generating an identifier for the actor, establishing grounds for authenticating the actor, delivering to the actor any data, tokens, or hardware the actor needs, and training users or software maintainers in the use of the selected technique. Each of these procedures has associated costs that add to the bottom-line costs of establishing or maintaining supported functions. Cost should in general be minimized. This requirement is often in conflict with enterprise accuracy requirements.

Minimize Changes Needed to Existing System Infrastructure

System infrastructure includes equipment, facilities, people, and procedures. System infrastructure support for I&A includes both system-wide support and support at each connection point where actors interact with I&A services.

Changes to existing infrastructure or addition of new infrastructure have associated costs. For example, new equipment costs money to acquire, absorbs employee time to install, and carries maintenance costs. All these costs add to the bottom-line costs of establishing or maintaining supported functions, and in general should be minimized. This requirement is often in conflict with minimizing enterprise accuracy requirements.

Minimize Costs of Maintenance, Management, and Overhead

I&A is a business procedure that can require very substantial time and effort to maintain and manage. All these costs add to the bottom-line costs of running the business and in general should be minimized. This requirement is often in conflict with accuracy requirements.

Protect I&A Service and Assets

I&A assets, especially authenticators and related data, are vulnerable to theft or disclosure. The I&A service itself needs protection, including confidentiality and integrity of I&A data, availability of the I&A process, and accountability for I&A service-related actions. This requirement is supportive of accuracy requirements but is often in conflict with ease of use.

Variations Across Sets of Requirements

The specific values of requirements, and the relative importance of each requirement, vary in different use situations. The use situations given in the Problem section illustrate some of these differences. For example:

- I&A results used in granting on-line access to highly-sensitive enterprise information assets would be likely to place high importance on avoiding false

rejections and protecting I&A assets, and lesser importance on minimizing cost and effort to use.

- I&A results used in tracking who is downloading information or products from publicly-available enterprise Web site would be likely to place high importance on minimizing cost and effort to use, and lesser importance on avoiding false rejections.

Implementation

This section first provides further 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 I&A service is needed.

   Ensure that the domain has been identified and scoped. Typical I&A domains include an information system, physical facility, network, portal, or entire enterprise. Other constraints may bound the domain—for example, the I&A requirements for entering a designated facility during normal work hours may differ from the requirements outside business 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 I&A, I&A needs, enterprise constraints, and priorities. You can find a general candidate set of factors in Table 7.2.

3. Specify I&A requirements for the target I&A domain.

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

4. Define the relative importance of specific requirements.

   The association of factors and requirements is discussed below.

Factors in Determining Relative Importance

Table 7.2 presents factors for judging the relative importance to the enterprise of the generic I&A requirements that were identified in the Solution section. For each requirement, the table describes how the factors affect the relative priority of the requirement.

Table 7.2 Factors affecting relative importance of I&A requirements

GENERIC REQUIREMENT	FACTOR	IMPACT ON PRIORITY
Accurately detect imposters	Potential cost to the enterprise if a link is made with an identifier to which the actor is not entitled (for example, could be used to give access to assets)	This requirement should have increased priority if inability to detect imposters could cause significant damage to the enterprise or system.
Accurately recognize legitimate actors	Existence of time-critical functions where access is controlled based on actor identifier, potential cost to the enterprise if controlled critical functions are not performed in a timely manner.	This requirement should have increased priority if rejection of legitimate actors for time-critical functions could cause significant damage to the enterprise or system.
	User base sensitivity to temporary denial of service. potential cost in dollars or good-will to the enterprise if users become annoyed	This requirement should have increased priority if rejection of legitimate actors could occur to the point of significant denial of service and user annoyance.
Minimize mismatch with user characteristics	User experience	This requirement should have increased priority if the I&A service could cause significant user frustration by not accommodating user experience level, whether novice or sophisticated.
	User base membership (employees, partners, public, software)	This requirement should have increased priority if the I&A service could cause security risks or significant user frustration by not supporting all user categories, such as employees versus partners.
	User location (local, remote)	This requirement should have increased priority if the I&A service could cause security risks or significant user frustration by not supporting all user locations, such as local versus remote.
	User mobility (fixed or mobile locations, fixed or variable devices)	This requirement should have increased priority if the I&A service could cause security risks or significant user frustration by not supporting user mobility, such as fixed versus mobile locations.
Minimize time and effort to use	Frequency of use	This requirement should have increased priority if the I&A service has heavy use.

Table 7.2 Factors affecting relative importance of I&A requirements (*continued*)

GENERIC REQUIREMENT	FACTOR	IMPACT ON PRIORITY
	User base characteristics	Inability of some users, such as handicapped users, to perform I&A may require changes to the business model. An I&A service that is difficult to use and requires more time may increase the potential costs in money or good-will if users become annoyed. Both should increase the priority of this requirement.
Minimize risks to user safety	Relevant statutes and enterprise policy	Statutes or policy may mandate this requirement, in which case it would in effect have top priority.
	Potential liability of enterprise for injury (for example damage to eye in retinal scan)	This requirement should have increased priority if the I&A service poses significant risk of incurred costs, and negative publicity, from users injured performing I&A.
Minimize costs of per-user setup	Number of users in general terms (hundreds, thousands, millions)	The existence or projection of a large number of users should increase the priority of this requirement.
	Volatility of user base	The existence or projection of a large turnover rate among users should increase the priority of this requirement.
	Existing user knowledge and skills	The existence or projection of a large proportion of novice users should increase the priority of this requirement, while a large proportion of experienced users should decrease its priority. However, for I&A, this factor is usually a minor one in either case.
Minimize changes needed to existing infrastructure	Number of connection points	A large number of connection points for the I&A service should increase the priority of this requirement, because each connection point may need an associated change.
	Predicted restructuring of existing infrastructure	If the infrastructure is already scheduled to be changed for other reasons, this requirement will have reduced priority.

Table 7.2 Factors affecting relative importance of I&A requirements (*continued*)

GENERIC REQUIREMENT	FACTOR	IMPACT ON PRIORITY
Minimize costs of maintenance, management, and overhead	Ability to rely on users properly to protect data or hardware entrusted to them	This requirement should have decreased priority if the users are knowledgeable and trustworthy. However, this assumption has some risk.
	Volatility of user base	The existence or projection of a large turnover rate among users should increase the priority of this requirement.
Protect I&A assets	Cost and risk of authenticator theft	This requirement should have increased priority if the cost and risk of theft of an authenticator, such as a password, is relatively high.
	Cost and risk of I&A service being unavailable	This requirement should have increased priority if the cost and risk of I&A being unavailable is relatively high.

Example Resolved

Samuel the systems engineer and Edward the enterprise architect identify each situation from the museum example above as a separate domain, with a separate set of requirements. The first domain for which they specify I&A requirements is that of the museum employees who access the museum information systems. Table 7.3 shows the requirements they specified for this domain. The first column contains two sets of information: the generic requirement, followed by the specific requirement for the museum. The second column presents the relevant factor for the requirement in this domain, and the third column discusses the resulting importance of each requirement.

Table 7.3 Resolving requirements for museum information system I&A

GENERIC/SPECIFIC REQUIREMENT	FACTOR	IMPORTANCE FOR MUSEUM
Accurately detect imposters. The I&A service shall have a minimum certainty of 0.9999 (shall have no more than 1 false acceptance out of 10000 I&A claims of imposters).	Potential costs of not detecting an imposter	All I&A services for workstations in physical asset display and research work areas must satisfy this requirement. The museum considers this to be extremely important.

Table 7.3 Resolving requirements for museum information system I&A (*continued*)

GENERIC/SPECIFIC REQUIREMENT	FACTOR	IMPORTANCE FOR MUSEUM
Accurately recognize legitimate actors. The I&A service shall have a maximum false rejection rate of 0.02 (shall deny no more than 1 actor out of 50 I&A claims of entitled actors).	Existence of time-critical functions	This is a moderate level of concern for the museum wing, as they prefer to incur the costs of hampered staff than to falsely assert the identity of an actor.
	User base sensitivity to temporary denial of service	N/A
Minimize mismatch with users. The I&A service shall support information system users with these characteristics: users are employees interacting with museum information systems, there are local and remote user locations, and the user locations are fixed.	User base membership (employees, partners, public, software)	The museum considers this a moderate concern. Only identified and authenticated actors will be able to log on to the information system. No anonymous users.
	User location	All user locations are known.
	User mobility	All I&A services will have fixed locations.
Minimize time and effort to use. The I&A service shall be easy to use.	Frequency of use	Museum users will not be required to perform multiple log-ons. Training will be provided to ensure workstations are logged off. The museum does not consider this a significant requirement.
	User base characteristics	The museum considers this a moderate concern related to staffing.
Minimize risks to user safety. The I&A service shall provide adequate safety.	Relevant statutes and enterprise policy	Statutes and policy do mandate this requirement for the museum.
	Vulnerability of enterprise to negative publicity	N/A

Table 7.3 Resolving requirements for museum information system I&A (*continued*)

GENERIC/SPECIFIC REQUIREMENT	FACTOR	IMPORTANCE FOR MUSEUM
Minimize costs of per-user setup. The I&A service set-up cost per person shall be as small as possible, and in any case shall be less than $50 per person.	Number of users in general terms	The museum's user base will be restricted to identified and authenticated users. Costs for I&A will be per workstation.
	Volatility of user base	The museum considers this a moderate concern as the rate of staff turnover is not high.
	Existing user knowledge and skills	As noted, the museum intends to provide user training to reduce costs.
Minimize changes needed to existing infrastructure. The I&A service shall be able to interface with existing components from the parent enterprise.	Existing support contracts	The museum considers this requirement extremely important. The I&A for this museum wing must be able to interface with existing components from the parent enterprise.
	Number of connection points	As above, museum costs will be per workstation, the same as the parent enterprise.
	Predicted restructuring of existing infrastructure	Any future infrastructure changes will occur under the parent enterprise funding profile.
Minimize costs of maintenance, management, and overhead. The I&A service shall be cost effective with respect to maintenance, management, and overhead.	Ability to rely on users	User training will be provided.
	Volatility of user base	The museum considers this a moderate concern, as the rate of staff turnover is not high.

Table 7.3 Resolving requirements for museum information system I&A (*continued*)

GENERIC/SPECIFIC REQUIREMENT	FACTOR	IMPORTANCE FOR MUSEUM
Protect I&A assets The I&A service shall protect its security assets, such as passwords.	Cost of authenticator theft	The museum considers this a very important requirement, since it could put physical assets at risk.
	Cost of I&A service being unavailable	The museum will need to address multiple back-up plans for loss of I&A service.

Samuel and Edward determine that the most important I&A requirements for the museum are:

1. Accurately detect imposters
2. Minimize risks to user safety
3. Minimize changes needed to existing infrastructure
4. Protect I&A assets

Known Uses

The general I&A requirements and the process of specifying I&A requirements described in this pattern represent a consolidation of MITRE Corporation's experience in working with multiple customers over several decades. The approach is generally used informally by those customers, as opposed to being codified or published. However, some discussions of I&A requirements exist. Examples include:

- [OMB2003] is a US government policy for electronic authentication of individuals participating in on-line transactions. It discusses some of the non-functional requirements identified in this pattern, such as cost and user burden. [NIST2004] provides technical guidance for this policy.
- [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 establish and verify a claimed user identity.
- [SEI2004] is a risk-based technique to elicit authentication requirements for electronic transactions. It includes the process of defining context, scope, and nonfunctional I&A requirements.
- [Firesmith2003] describes functional I&A requirements (false positives and false negatives), and discusses I&A domains in terms of requirements scope.

Consequences

You may expect the following benefits from applying this pattern.

- The pattern fosters explicit definition of I&A domains and a clear connection of requirements to I&A domains. This increases understanding of the full set of domains that are involved in I&A and understanding of the scope of each set of requirements.
- It facilitates conscious selection of I&A requirements, so that decisions about selecting I&A 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 I&A, which makes it difficult for valid users, and at the same time it helps to avoid weaker than necessary I&A, which makes it easy for imposters to defeat and therefore provide inadequate protection.
- It results in documentation of I&A requirements that communicates to all interested parties, and also provides information for security audits.

The potential liabilities of applying this pattern are:

- It requires an investment of resources to apply the pattern, including time to analyze domains and I&A 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 way as noted above.
- Specific circumstances might not be covered by generic I&A 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 I&A requirements can differ throughout an organization. This may make it difficult to reach agreement on priorities between 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 is typically to decide what type of I&A to use. If you have made a decision to use only automated I&A, you can apply AUTOMATED I&A DESIGN ALTERNATIVES (207).