7.2 Automated I&A Design Alternatives

This pattern describes alternative techniques for automated I&A, as opposed to procedural or physical I&A. It helps you to select an appropriate I&A strategy that consists of a single technique, or a combination of techniques, to satisfy I&A requirements. Techniques considered include password, biometrics, hardware token, PKI, and I&A of unregistered users.

Also Known As

Decision Tradeoffs for Automated I&A [HHR+02].

Example

Indiana Jones, a museum employee, needs to gain access to the museum intranet while collecting artifacts for the museum from around the world. He wants to check his e-mail abroad and also access the museum's database to evaluate a found artifact. From Jones' perspective, the most important requirements for this I&A service are to support I&A from remote locations and to be easy to use. From the perspective of Samuel the museum systems engineer, the most important requirements for this I&A service are to have high accuracy, especially to reject attempts by non-employees to gain access to the intranet, and to limit I&A overhead. Samuel and his systems engineering group have used I&A REQUIREMENTS (192) to define all four of these intranet I&A requirements as high priority. Now Ivan the intranet architect needs to select an I&A service to satisfy these requirements. The choices available to Ivan are many. They include identifier and password, PKI certificates, multiple biometrics options, and a hardware token with a one-time password. How can Ivan choose among the alternatives?

Context

The person applying this pattern understands the requirements for I&A, along with their relative importance—for example, from the results of applying I&A REQUIREMENTS (192).

A decision has been made to use automated I&A[1].

[1] In the remainder of this pattern, the term 'I&A' is intended to mean automated I&A, as opposed to physical or procedural I&A, such as showing a badge to a guard at the front door.

Problem

I&A is a common need for systems and enterprises. Multiple techniques exist for achieving I&A. Different techniques emphasize different types of authenticators. No one technique is the best in all situations. Trade-offs and weighting are typically necessary, because in general the techniques have differing and often complementary strengths and weaknesses. For example, PKI provides high accuracy, but has relatively high infrastructure and cost impact, while passwords provide less accuracy, but have low infrastructure and cost impact.

In addition, certain combinations of techniques can produce an I&A strategy that in some circumstances satisfies requirements better than any of the individual techniques. For example, a combination of password and hardware token is typically stronger than either individual technique, because each compensates for a weakness of the other.

A common perspective for comparing and combining techniques is the following categorization:

- Something you know, for example a password.
- Something you have, for example a hardware token.
- Something you are, for example a biometric characteristic such as an iris image.
- Recently a fourth category has emerged: where you are, for example, derived from either your IP address or through the use of GPS, which is now included in some cell phones and PDAs. This is an additional kind of information available for authentication.

An I&A strategy may be influenced by the selection of strategies for other I&A domains within an enterprise. The enterprise may find it more efficient—in terms of cost, training, and maintenance—if all I&A domains that have similar requirements use the same strategy. For example, the enterprise may decide that the I&A used in granting out-of-hours physical access to all enterprise facilities throughout the country should use the same technique, such as biometrics.

Using a single technique for I&A in an organization is attractive, for example for achieving single sign-on (SSO). On the other hand, using a single technique is also dangerous, because it is a single point of failure, thus violating the ‘defence in depth’ principle (see Chapter 15). For example, if you are an imposter and your identity claim is accepted, you may be given access to multiple critical resources.

How can a strategy for I&A be selected that satisfies I&A requirements?

Based on the foregoing discussion, we can summarize the forces that influence selection of a strategy that balances techniques to satisfy I&A requirements:

- Some techniques satisfy some I&A requirements better than others.
- In many cases certain combinations of I&A techniques can satisfy requirements better than any individual technique. A common strategy is to combine

techniques from two or more of these categories: something you know, something you have, something you are, and where you are.

- An I&A strategy may be influenced by the selection of strategies for other I&A domains within an enterprise.
- Using a single technique for I&A across an organization may be efficient, but it is also dangerous, because it is a single point of failure.

Solution

Systematically review the characteristics of the available I&A techniques, and select a strategy that consists of one or more techniques. Proven techniques include user ID/password, hardware token, biometrics, PKI, and I&A of unregistered users. These are not the only techniques that exist, or that will exist in the future, but they are the techniques described in this pattern.

The selection process is typically performed by a person or team serving in the role of system architect, security architect, or enterprise architect, depending on the nature and scope of the domain. The process includes several activities: explicitly assembling the necessary inputs for decision making is an important first step. Inputs include a definition of the I&A domain or scope of the strategy, I&A requirements, and the general values of factors for each I&A technique. The inputs are then used to define specific technique profiles for the chosen domain. With this information, you can compare the I&A requirements with techniques to determine the best matches. Finally, if no individual technique adequately matches the requirements, you can look at combinations of techniques.

Implementation

This section first provides further detail on the process that was summarized in the Solution section, then presents information on technique profiles. Finally, considerations are given for combining techniques and selecting a strategy.

Process Guidelines

The selection process includes the following steps:

1. Assemble the necessary inputs for decision making.

   Two of the inputs are a definition of the I&A domain or scope and the I&A requirements. If you have applied the pattern, both of these inputs should be available. The requirements should include enterprise constraints, and an indication of the importance of each requirement—for example via ranking, weighting, or criticality indicators. The third input is a technique factor profile summary, that is, general values of factors for each technique. Table 7.4 on page 213 provides a summary that you can use for certain I&A techniques.

2. Define the specific technique profiles for this domain.

   The next step is to specialize the general technique factor profile for your specific I&A domain. You can use the technique profiles discussion below to tailor the value of each technique in your domain. For example, if your domain excludes software actors, then satisfaction of the requirement to support a variety of user types (that is, the entry for User Types) is high for all techniques with respect to your domain.

3. Compare the I&A requirements with individual technique profiles.

   If one technique satisfies the requirements, select that technique as the I&A strategy: if not, perform step 4.

4. If no single technique is adequate, look at combinations of techniques.

   Combine techniques that have complementary strengths and weaknesses. You might benefit from the discussion of combinations and the overall organizational perspective that follows Table 7.4.

Technique Profiles

I&A techniques differ in what they use for IDs, identifiers, and authenticators, as well as other characteristics that affect their selection. A description of each technique is given. The purpose of this section is to define their comparative characteristics. Each I&A technique has a characteristic profile with respect to factors affecting the ability of the technique to satisfy the requirements. The profile for each technique is discussed here and summarized in Table 7.4.

User ID/Password

This technique generally scores high on cost effectiveness and usage requirements, but lower on reliability and protection of passwords. Password's ability to avoid confirming imposters is medium at best, because passwords can be obtained through theft or other means. This ability depends on good password practice—for example, the use of hard-to-guess passwords, and not recording passwords in easy-to-find locations. Password's ability to avoid denying legitimate users depends on the likelihood of remembering passwords: good passwords can be somewhat difficult to remember.

Regarding user types, passwords as they are typically defined may not be suitable for software actors. A common belief is that passwords are easy to use. It is true that poor password practice is easy. Good password practice is harder to achieve, but it can be made easier through schemes such as one-time passwords, which is described below.

Biometrics

The biometrics technique profile varies more than other techniques. This is due to the fact that multiple biometric techniques exist. A general profile is described here, and the various biometric techniques are described further in BIOMETRICS DESIGN ALTERNATIVES (229).

Biometric techniques have the potential for high reliability, depending on the type of biometric selected. On the other hand, biometric techniques generally cost more and are not as easy to use as some other techniques. Biometric techniques often do well in recognizing legitimate users. However, environmental or aging factors may affect biometric readings. Such factors include poor lighting, sunglasses, facial hair, and change due to injury or disease.

Biometrics techniques are not suitable for software actors. Some biometric techniques may not be suitable for some types of mobile computing (for example cell phones). Safety depends on the type of biometric technique: retinal scans can cause damage to retina, so its safety is low. The cost is increased due to the need for biometric devices or scanners, as well as additional processor, storage, network loads and in some cases additional processing software. It is possible to steal biometric information, which has the potential for severe problems for a user. It is difficult and rather painful to change your biometric characteristics, such as fingerprints.

PKI

This technique depends somewhat on the population to which it is applied. It can score very highly on reliability with a relatively sophisticated user base, but has high cost. It may not be suitable for world-wide computing—that is, from locations where communications to registration servers have low availability. You not only have to trust the third party issuing the certificates, you also have to trust your computer hardware and software not to compromise your private keys or use weak encryption. In addition, you have to trust yourself or your employees to be able to validate the certificates and to actually do so.

Infrastructure impact is very high, including software development practices. It has moderate to high management costs, because of the third party involved. A PKI can work well with a defined user population where an established body issues certificates and carries a directory of public keys related to the individuals and organizations within that closed community. For example, it seems to work well within the Swiss medical community.

Hardware Token

The reliability of this technique can vary. The ability to avoid confirming imposters depends on the degree of protection of the token. Reliability is high if combined with password for use of the token. Stand-alone token ability to avoid denying legitimate users is high. If combined with password, this ability is medium, because of the possibility of mis-typed or forgotten passwords. Token techniques are not suitable for software actors. Some token types may not be suitable for some types of mobile computing (for example cell phones). Some types of tokens require moderate to high costs per connection, because they use token readers, while other types may only require installation of additional software. Authenticator protection depends on users to report lost tokens.

Unregistered Users

This technique generally scores highly on ease of use and cost effectiveness, but is low on reliability. The technique scales up to a very large user base. It is not suitable for software actors.

In Table 7.4, the requirements listed in the requirements column are described in detail in I&A REQUIREMENTS (192). The value or range of values indicates the extent to which a technique satisfies an I&A requirement. High indicates high satisfaction of the requirement, and Low indicates low satisfaction.

To determine the I&A technique(s) that will meet the I&A needs, a general approach is to compare the technique profiles with your results from applying I&A REQUIREMENTS (192) to find a technique that is most compatible with your specific requirements.

Considerations for Combining Techniques

From Table 7.4 it is clear that different techniques have different strengths and weaknesses. None of the techniques resolves all forces, and each one resolves certain forces better than others. In many situations, no single technique satisfies all important requirements. However, some techniques complement others, so that certain combinations of techniques can satisfy more requirements. It is often useful to combine techniques from different categories: what you know, what you have, what you are, where you are.

A common example of combined techniques is a hardware token combined with a user ID/password. Typically, a small hand-held device is synchronized with the target system's authentication scheme and displays a one-time password (OTP). To access the target system, the user enters an assigned user ID and password or PIN (personal identification number) followed by the OTP displayed on the hand-held device. Some implementations, such as SecurID are time-driven, that is, the OTP changes periodically, perhaps every minute. Other schemes are event-driven, using a button to press to get the next OTP. The latter have fewer problems with re-synchronization. The advantage of this strategy of combined token and password/PIN techniques is that it helps to prevent the replay of a compromised password. This combination increases accuracy by avoiding confirming imposters more than that of either individual technique. It also improves the protection of authenticators—unless of course you write the PIN on the token! This improvement is because the two part authenticator (OTP

Table 7.4 Summary of I&A technique profiles

REQUIREMENT	USER ID/ PASSWORD	BIOMETRICS	PKI	HARDWARE TOKEN	UNREGISTERED USERS
Avoid confirming imposters	Med–Low	High–Med	High	Med–High	Med–Low
Avoid denying legitimate users	Med	High–Low	High	Med–High	Med–Low
User types	Med–High	Med–High	High	Med–High	Med–High
User location	High	High	Med	High	High
User mobility	High	Low–Med	High	Low–Med	High
Easy to use	Med–High	Med	Med	High–Med	High
Speed of use	High	Med–High	Med	High	High
Safety of use	High	Low–High	High	High	High
Cost effective per user	High	Low–High	Med–Low	Med–High	High
Cost effective per connection	High	Low	High	Low–High	High
Infrastructure compatibility	High	Med–Low	Low	High–Med	High
Cost effective maintenance	High	Med–Low	Med–High	Med	High
Protection for authenticators	Low–Med	Med	High	Med–High	Med
Availability	High	Med–High	Med–High	Med–High	High

and PIN) means that an impostor must now obtain both parts, using different means, in order to fool the system. This strategy illustrates the technique of combining something you know (the password) with something you have (the token).

Other Considerations for Selecting a Strategy

While the scope of this pattern is the selection of a single strategy for one I&A domain, this decision does not occur in a vacuum. Decisions made about strategies in other similar I&A domains within the enterprise may influence the decision for a given I&A domain. A trade-off is involved in these decisions between a homogeneous and a heterogeneous approach across the organization. In a homogeneous approach, you use the same technique everywhere. The benefits of this include ease of single sign-on (SSO), efficiency of cost, training, and technical support, and establishing a standard for future application developments. On the negative side, this approach weakens the defence in depth achieved.

In a heterogeneous approach, you explicitly choose different I&A mechanisms for different I&A domains. The primary benefit of this is stronger defence in depth. On the negative side, this approach makes SSO more difficult and loses the efficiency of cost, training, and technical support. A small example of enforced heterogeneity is the Frontdoor product that is provided for HTTP and FTP. Since the FTP password is sent in plain text over an unencrypted TCP connection, the software requires a password that is not the same as the password for HTTP connections that are protected by SSL connections. If these passwords were the same, the 'weak' FTP-password would be the weak link for the (presumed) secure SSL-channel.

Example Resolved

How can Ivan the architect apply this pattern solution for I&A support of remote access to the museum intranet? The most important requirements for this museum I&A component are to have high accuracy, especially the ability to detect non-employees, to be easy to use, provide strong support of I&A from remote locations, and limit overhead. Based on the technique profiles, the high accuracy requirement suggests that PKI would be best, and biometrics and tokens may also be candidate techniques. The ease of use and low overhead requirements indicate that biometrics and PKI are not good candidates. Therefore, of the individual techniques, a token appears to be the best one, but it is not optimum.

To obtain a solution closer to optimum, Ivan considers combinations. He concludes that combining password and token techniques gives the best overall match with requirements, because the combination increases accuracy and protection, as discussed above in considerations for combining techniques. The combination also achieves the ease of use desired by Indiana Jones when he needs to log in from some exotic location. Ivan therefore chooses this combination as the I&A strategy for remote access to the museum intranet.

Known Uses

The approach to selection of I&A described in this pattern is 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. One discussion of trade-off factors for selecting an I&A strategy is presented in [Smith2002].

The individual techniques considered in this pattern are widely known and used. Passwords have been ubiquitous for decades in information systems. Hardware tokens are often used for remote access, and a common strategy is to combine a token with a pin or password (for example, the MITRE Corporation uses this strategy). Biometrics and PKI are becoming more widely used.

Consequences

The following benefits may be expected from applying this pattern.

- The pattern fosters engineer and manager awareness of the elements of the decision needed on selecting I&A techniques.
- It facilitates conscious and informed decision making about I&A to support identified I&A requirements, as well as clear traceability to requirements
- It encourages better balance among competing I&A selection forces and factors, by matching technique profiles to requirements in the context of your specific domain. The result is increased likelihood that an I&A technique will be selected that satisfies your most important requirements.
- It provides some assistance on how you can combine I&A techniques to provide a complete I&A service.
- It facilitates broader enterprise optimization by promoting integration of I&A choices across multiple domains and systems across the enterprise.

The following potential liabilities may result from applying this pattern.

- It requires an investment of resources to apply the pattern, including time to analyze I&A mechanisms.
- This pattern focuses on certain selected I&A techniques. Using the pattern may mean that other techniques applicable to your specific domain are ignored, and a sub-optimum strategy may be selected. You can mitigate this by explicitly bringing other selected techniques into the decision process.
- Perception of identification and authentication (I&A) needs can differ throughout an organization. This may make it difficult to reach agreement on priorities of I&A and therefore difficult to select a I&A mechanism. On the other hand, bringing such disagreements to the surface may be a benefit, because then they can be properly discussed and resolved. This is true of individual strategies for a given domain. It is even more true of organization-wide coordination of I&A strategies-for example, by having different domains use different I&A techniques.

See Also

A discussion of trade-off factors for selecting an I&A strategy is presented in [Smith2002].

The registration or enrolment function complements this pattern. The operation of most I&A techniques, and in this pattern all techniques except UNREGISTERED USERS I&A REQUIREMENTS (67), require that the domain of users for which I&A is to be performed must first be registered or enrolled, to obtain the independent user information. Although no registration pattern is described in detail this book, the registration function is part of the larger I&A picture (see Chapter 5, *The Security Pattern Landscape*).