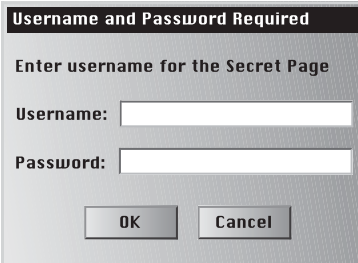


7.3 Password Design and Use

This pattern describes security best practice for designing, creating, managing, and using password components in support of I&A REQUIREMENTS (192). This pattern can aid three audiences: engineers, in selecting or designing commercial products that provide password mechanisms, administrators, in the operation and management of password mechanisms, and users, in improving their selection and handling of passwords.

Example

Employees of the museum need to gain access to the museum intranet, which is based on passwords. Enforcement of security policy has been lax, and it has been common practice for employees to write down passwords and leave them by their workstations, or even tape them to the display monitor. As a result, several incidents have occurred in which unauthorized staff and even visitors have gained access to sensitive information. The system administrators want to correct this problem, specifically to create good passwords and keep them secure. There are two situations that require passwords as part of I&A whose results are used for access control. First, a low level of security is needed for I&A used to gain access to the overall intranet. Second, a high level of security is needed for I&A used to gain access to sensitive information, including employee salary data.



Context

A password mechanism has been selected for user authentication on a specified segment of an information system. 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).

Problem

How can passwords be created, managed, and used in a manner that retains password accessibility for their owners, but renders the passwords inaccessible to imposters?

In addition to forces relating to issues that apply to all I&A authenticators, the following forces specifically affect password practice:

- Stolen or guessed passwords can be used to masquerade as another person, which leads to false positives, that is, falsely confirming an unauthorized identity
- If passwords are stolen or compromised, assets whose protection relied on the confidentiality of the passwords can be damaged
- People need to remember their passwords in order to use them
- Passwords that are difficult to guess tend to be difficult to remember, which leads to false negatives, that is, falsely denying an authorized identity
- Passwords that are recorded can be intentionally or inadvertently discovered by someone else
- A person typically has many contexts in which a password is needed
- Using a single password in all contexts increases the potential scope of damage from password theft
- Using a different password in each context increases the difficulty of remembering each one, which in turn increases the pressure to record each one, reducing the protection of the passwords
- Passwords that are not changed periodically become increasingly susceptible to theft

Solution

Ensure that passwords are properly designed and defined, properly used and properly protected. More specifically, consider several factors that address each area—for example, consider the length of the password during design and definition. Determine how the factors can be used to best satisfy the I&A requirements for the specific domain being considered, such as a specific network or information system.

The following factors should be considered:

Design and Definition of Passwords

- Composition: the characters that are usable in a valid password
- Length range: the minimum and maximum acceptable number of characters in a valid password
- Source: the entities that can create or select a valid password from among all acceptable passwords

Use of Passwords

- Lifetime: the maximum acceptable period of time for which a password is valid
- Ownership: the set of individuals who are authorized to use a password
- Entry: acceptable methods by which a password may be entered by a user
- Authentication period: the maximum acceptable period between any initial authentication process and subsequent re-authentication processes during a single session

Protection of Passwords

- Distribution: acceptable methods for transporting a new password to its owner(s) and to all places where it will be needed
- Storage: acceptable methods of storing a valid password during its lifetime
- Transmission: acceptable methods for communicating a password from its point of entry to its point of comparison with a stored, valid password

Best practice details on each of these factors, as well as recent evolution of thinking on what is best practice, are provided in the Implementation section. See figure on page 220.

Structure

The general relationships among I&A requirements, password constraints, and passwords are illustrated in the figure above. A set of requirements for the specific domain under consideration clearly influences password constraints, which consist of several factors to be considered when selecting or designing passwords, as identified in the figure. The password constraints are used by engineers and administrators in building or selecting password systems, or configuring and managing passwords. The constraints constrain passwords that are defined by users.

Implementation

This section discusses classical best practice with respect to each of the factors introduced previously. It then briefly describes how some of the classical guidance is evolving to reflect the influence of the changing information technology environment.

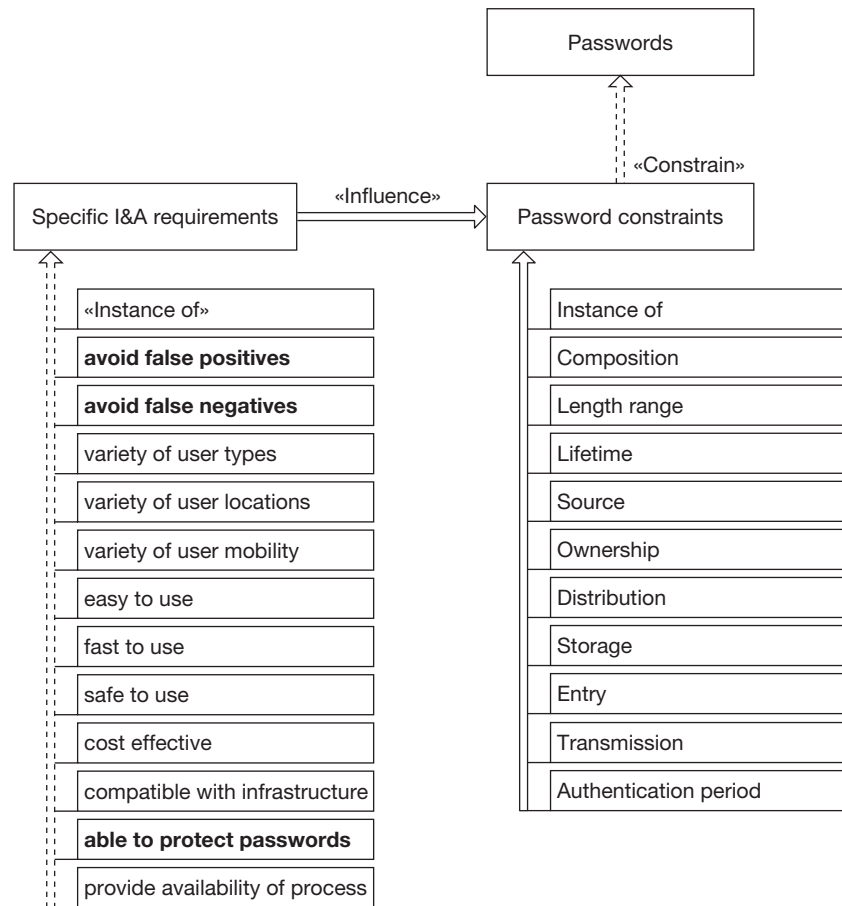
1. Composition.

Composition is the set of acceptable characters usable in a valid password.

Consider the following good practice:

Passwords should be composed from a defined set of ASCII characters.

The password mechanism should verify that only characters in the defined set have been generated or selected whenever a password is created or changed.



Password solution structure

Include a digit or punctuation.

Use upper and lower case.

Choose a phrase or combination of words to make the password easier to remember.

Two words separated by a non-letter non-digit character is acceptable.

Use different passwords on different machines.

When changing a password, don't reuse passwords or make only minor variations such as incrementing a digit.

Avoid the following bad practice:

Do not use your account name or account data.

Do not use any word or name that appears in any dictionary, reference or list regardless of case changes, and especially do not use character strings that appear in password cracking tools' word lists or bad password lists.

Do not use the following variations: phrases and slang with or without white space:

- Any mythological, legendary, religious or fictional character, object, race, place or event
- Acronyms
- Alphabetic, numeric or keyboard sequences—many such sequences are included in cracking tools word lists
- Titles of books, movies, poems, essays, songs, CDs or musical compositions

Do not vary the character sequences obtained from any of the foregoing items. Specifically, do not use any of the following methods:

- Prepend or append symbols, punctuation marks or digits to a word
- Use words with some or all the letters reversed
- Use conjugations or plurals of words
- Use words with the vowels deleted
- Use only the first or the last character in uppercase
- Use only vowels in uppercase
- Use only consonants in uppercase

Do not use any personally-related information (see below).

Do not use a publicly shown example of a good password.

Do not use vanity license plates.

Do not transliterate words from other languages.

Do not repeat any character more than once in a row.

Using personally-related information is poor practice. The most common examples of personal information include: names and initials, account name, names of immediate family members, names, breeds or species of pets, birthday, family member's birthdays, vehicle make, model, year, hobbies, interests, and job title. All permutations or combinations of the foregoing should also be avoided.

2. Length range.

Length range is the set of acceptable lengths of passwords, defined in terms of a minimum and maximum number of characters in a valid password.

Consider the following good practice:

Passwords should have a length range, selected by the system manager and security officer, having a number greater than or equal to four as the minimum length and a maximum length. The maximum length should reflect the recognition that the average person can easily remember a maximum of seven items.

The selected password composition and length range should allow for a minimum of 10,000 possible passwords, to make passwords less guessable. The selected password length range should provide a level of protection commensurate to the value or sensitivity of the resources or data it protects. A pass phrase—that is, a character sequence longer than the acceptable length of a password—should be transformed into a virtual password of acceptable length for storage.

The password mechanism should verify that only passwords having a length within the acceptable length range are generated or selected whenever a password is created or changed.

3. Source.

Source is the set of acceptable entities that can create or select a valid password from among all acceptable passwords.

Consider the following good practice:

The source of passwords should be selected by the Security Officer and System Manager, and should be one or more of the following: user, security officer, or automated password generator.

All passwords that may be included in a new system when it is delivered, transferred or installed (for example passwords for the operator, system programmer, maintenance personnel or security officer) should be immediately changed by the security officer to one of the following:

- (a) Passwords that are invalid to the password system
- (b) Random passwords that may be subsequently changed
- (c) Valid passwords that are owned by authorized users of the system

Passwords created by the security officer for new users of the system during initial system access should be selected at random from all acceptable passwords. Default passwords or formatted passwords related to the new user's identity or assignment should not be used.

Users who create or select their own personal password should be instructed to use a password selected from all acceptable passwords at random, if possible, or to select one that is not related to their personal identity, history or environment.

Passwords selected or created by users or the security officer should be tested by the password system to assure that they meet the specifications of composition and length established for the system before they are accepted as valid passwords.

4. Lifetime.

Lifetime is the maximum acceptable period of time for which a password is valid.

Consider the following good practice:

Passwords should have a maximum lifetime of one year.

Passwords should have the shortest practical lifetime that provides the desired level of protection at the least possible cost.

Passwords should be replaced quickly if compromise of the password is suspected or confirmed.

Passwords should be deleted or replaced with an invalid password when an owner is no longer an authorized system user.

Passwords forgotten by their owner should be replaced, not reissued.

The password mechanism should allow the security officer, appropriately authenticated, to delete or replace a password.

The password mechanism should be capable of maintaining a record of when a password was created and changed.

5. Ownership.

Ownership is the set of individuals who are authorized to use a password.

Consider the following good practice:

Personal passwords used to authenticate identity should be owned (that is, known) only by the individual with that identity.

Each individual should be responsible for providing protection against loss or disclosure of passwords in their possession.

6. Entry.

Entry is the set of acceptable methods by which a password may be entered by a user for authentication or authorization purposes.

Consider the following good practice:

Passwords should be entered by the owner upon request by the password mechanism in a manner that protects the password from observation.

Users should be allowed more than one attempt to enter a password correctly to allow for inadvertent errors. However, the number of allowed password entry attempts—retries after incorrect password entry—should be limited to a number selected by the security officer. A maximum of three attempts is considered adequate for typical users of a computer system.

The response to exceeding the maximum number of retries should be specified by the security officer. The latter may include, for example, account lock-down, account suspension for a specified time, or account release by security officer only.

7. Authentication period.

Authentication period is the maximum acceptable period between any initial authentication process and subsequent re-authentication processes during a single terminal session.

Consider the following good practice:

Individual passwords should be authenticated each time a claim of identity is made, for example when logging on to an interactive system.

A system should have log-on time-outs established. That is, if there is no user activity for a specified period of time (the time-out period) the user is automatically logged off and must re-enter their password to continue work. Shorter time-outs offer better protection in theory, but may impact the business process unacceptably and try user patience to the point where users will find ways of bypassing I&A.

8. Distribution.

Distribution is the set of acceptable methods for providing (transporting) a new password to its owner(s) and to all places where it will be needed in the information system.

Consider the following good practice:

Personal passwords should be distributed from the password source in such a way that only the intended owner may see or obtain the password, for example in a separately-mailed envelope.

Passwords should be distributed in such a way that an audit record, containing the date and time of a password change, and the identifier associated with the password, but not the old or new password, can be made available to the security officer.

Passwords should be distributed from the password source in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner(s) and the protected-password system.

The password system that generates and distributes passwords should keep an automated record of the date and time of password generation and to whom it was distributed, but not the password itself.

9. Storage.

Storage is the set of acceptable methods of storing a valid password during its lifetime.

Consider the following good practice:

Stored passwords should be protected such that only the password mechanism(s) is authorized access to a password. Examples include:

- Most systems have a password file that can be legitimately read only by the log-on process
- Some systems separate the password file from the authorized user file
- Some systems encrypt passwords, either reversibly (two-way) or irreversibly (one-way) using a data encrypting key.

Passwords that are encrypted before they are stored should be protected from substitution—that is, protection should be provided such that one encrypted password cannot be replaced with another unless the replacement is authorized.

10. Transmission.

Transmission is the set of acceptable methods for communicating a password from its point of entry to its point of comparison with a stored, valid password.

Consider the following good practice:

Passwords that are transmitted between the place of entry and the location for comparison against a stored password should be protected to the degree specified by the security officer, and at least equivalent to the protection required for the entities, such as the system or its data, that the password is protecting.

Passwords used as encryption keys should be selected at random from the set of all possible keys (for example, 236 keys for the Data Encryption Standard) and used either as data-encrypting keys or key-encrypting keys, but not both.

Unencrypted passwords should be transmitted as ASCII characters if interchanged between systems, while encrypted passwords and virtual passwords should be transmitted either as 64-bit binary fields, or as the ASCII representations of the hexadecimal character set [0-9, A-F].

Discussion: Evolution in password thinking

As noted in [Smith2002], the classical password selection rules can be summarized as follows: the password must be impossible to remember and never written down.

This illustrates the limitation of passwords as authenticators, and is compounded by the large number of passwords typically needed by a single individual—for example, for different computers, networks, and Web sites. It can be argued that the set of passwords that simultaneously conform to all the classic rules is a null set. Because of this limitation, and because of the trend toward more network use, the prohibition against

writing down passwords is being reconsidered. The risk of having passwords compromised on the network has increased to the point where it significantly outweighs the risks of local compromise, that is, writing down passwords. One password guide [Geodsoft2002b] recommends recording sensitive passwords and protecting the recorded passwords, especially root or administrator passwords. This guidance may also apply when one person must remember a significant number of passwords. For example, multiple passwords could be stored and protected on a USB token.

[NIST800-63] defines four levels of assurance for authentication. Level 1 allows password challenge-response protocols, and does not require cryptographic methods. Level 2 allows passwords, but requires a secure authentication protocol and the use of cryptographic techniques. Level 3 requires at least two authentication factors, of which one can be a one-time password. Level 4 also requires multi-factor authentication, but does not allow passwords: both factors must be physical cryptographic tokens.

Example Resolved

The new museum wing's security officer, engineering team, and system manager determine that two different password systems are needed to deal respectively with the high and low security situations described in the Example and Problem sections.

1. Password system for low-protection requirements: I&A for access to museum intranet.

Value for each factor:

- Composition: Digits (0–9)
- Length range: 4–6
- Source: user
- Lifetime: one year
- Ownership: individual (personal password), group (access passwords)
- Entry: non-printing keypad
- Authentication period: each intranet session log-in, plus the end of each period of workstation inactivity that exceeds thirty minutes
- Distribution: unmarked envelope by post
- Storage: central computer on-line storage as plaintext
- Transmission: plaintext

2. Password system for high-protection requirements: I&A for access to sensitive museum data.

Value for each factor:

- Length range: 6–8
- Composition: full 95 character set
- Source: automated password generator within the authentication system
- Lifetime: one month
- Ownership: individual
- Entry: non-printing keyboards
- Authentication period: log-in and after five minutes of terminal inactivity
- Distribution: registered mail with receipt required
- Storage: encrypted passwords
- Transmission: encrypted communication with message numbering

Variants

Dirk Riehle and colleagues have defined a ‘Password pattern language’ that includes a few general security patterns and several specific password patterns [Riehle2002]. The language is a work in progress. Each pattern in the language addresses a very specific password issue such as a best practice item within the factors addressed in this pattern. For example, their `DICTIONARY WORD` pattern corresponds approximately to the ‘Choose a phrase or combination of words to make the password easier to remember’ item in this pattern under the composition factors.

Schumacher et al. introduced some password-related patterns [SRM03]. `USER AUTHENTICATION PASSWORDS` describes the general I&A approach that is based on passwords, a special case of ‘something you know.’ Another pattern, `PASSWORD QUALITY`, addresses the design and definition issues of passwords. Finally, there is also a general pattern that deals with `PASSWORD PROTECTION`. There are further related patterns that are used to implement password protection, namely ‘Physical Protection,’ a set of patterns that deals with `SECURING LOCAL NETWORKS` and a set of patterns that deal with `SECURING WIDE AREA NETWORKS`.

Known Uses

The factors are well-known, and passwords themselves are used in most information systems, including operating systems and file systems. The factors are taken from [FIPS112], and the good practice material is taken from [FIPS112], [NIST800-63], and [Geodsoft2002a]. [NIST800-63] is a partial replacement for [FIPS112].

Consequences

The benefits of applying this pattern are as follows:

- Applying this pattern results in increased protection of passwords and consequently higher accuracy of I&A.
- The potential number of false positives resulting from such things as password guessing is expected to be reduced.

The pattern also suffers from the following liability:

- Applying this pattern may lead you to conclude that passwords is the only I&A technique that needs to be used. It is often better practice to adopt a strategy that combines passwords with another technique.

You can find a discussion of password combination considerations in AUTOMATED I&A DESIGN ALTERNATIVES (207) earlier in this chapter.

See Also

Other approaches to password patterns include Dick Riehle's password pattern language in [Riehle2002] and the patterns presented by Schumacher et al. [SRM03]. Other techniques that are alternatives to passwords are described by the following patterns:

- BIOMETRICS DESIGN ALTERNATIVES (229)
- PKI DESIGN VARIABLES (66)
- HARDWARE TOKEN DESIGN ALTERNATIVES (66)
- UNREGISTERED USERS I&A REQUIREMENTS (67)

BIOMETRICS DESIGN ALTERNATIVES (229) is described in this chapter. Thumbnails of the other patterns can be found in Chapter 5, *The Security Pattern Landscape*.