# Password Patterns

This is a set of patterns describing how you could (maybe should) go about creating and handling your passwords in order to achieve practical security. These patterns were developed on a wiki.

## Overview



## Authors and contributors


Main authors:

- Dirk Riehle
- Joe Bergin

Contributors to the patterns:

- Sacha Brostoff
- Ward Cunningham
- Norm Kerth
- Nick Leaton
- Steve Metsker
- Eugene Wallingford

Also, there were some anonymous contributions.


These patterns are used or at least referenced in the upcoming Security Patterns book.

# Security Context

Synopsis: Approach security holistically.

---

It doesn't make much sense to have a complicated password scheme, but grant access to your hard disk or file system to everyone on the network.

Therefore, you need to choose your passwords in accordance with your overall approach to security. If necessary, plug other security holes while you develop your password scheme.

(As should be obvious then, this Password pattern language needs to be embedded in a larger context of system security. However, here we focus on passwords only and assume this context considered elsewhere.)

---

Next pattern: Stay Current And Ahead

Contributors: Dirk Riehle

# Stay Current And Ahead

Synopsis: Stay current or ahead.

---

Attacks are ever-changing, and even the patterns in this language may get out of date or constitute bad advice in an ever changing and evolving security and technology context. Thus, no scheme is perfect. However, many times, an attack may not be directed specifically at you or your accounts, but it may be geared towards gaining access to a system in general, and for the attacker, another person's account is as good as yours.

Therefore, stay current with respect to password attacks and what crackers to do gain knowledge. Choose your password scheme to be more difficult to crack than the average. This way you reduce the likelihood that you fall prey to an attack before some other account is cracked. How your password scheme relates to the average depends on your security needs.

To say it with Andy Grove: Only the paranoid survive.

---

Previous pattern: Security Context

Next pattern: Lay It Open

Contributors: Dirk Riehle, Joe Bergin

---

Is this pattern really just about being more **complicated** than usual? The idea of staying ahead of the pack implies an awareness of what's current, in particular about crackers' strategies for breaking passwords and the like. -- EugeneWallingford

Yes, I agree. Do you think this makes this pattern invalid? -- DirkRiehle

Not necessarily. You could broaden the pattern to address both complexity and current technique, which may result in a new pattern downstream. You could create separate patterns to deal with complexity and techniques. Or you could decide to maintain this pattern's focus on complexity, perhaps expanding on it, and simply choose a more representative name. -- EugeneWallingford

Not sure what you mean. I renamed the pattern, but I'm still not happy. The key issue is simply to detract attackers by letting them suspect/have easier prey some place else. -- DirkRiehle

---

There exists a very old method to hide important information. It was used by wise men to inform others. They used stories, which referred to daily events, but hidden in them was information for the knowledgeable persons. This method was used by the Sufis for instance. Using modern computer technology one could use a large piece of text and put into it the information, which one wants to hide. The algorithm for hiding could be very simple. -- AnonymousContributor

# Lay It Open

Synopsis: Lay open a complicated password scheme for public scrutiny.

---

Sometimes, you may think you have come up with a really clever password or security scheme, however, you haven't. Thus, flaws in your scheme may go unnoticed until you or a cracker recognizes them. Public exposure may help fix the flaws before they become a problem.

Therefore, lay open a complicated password scheme and expose it to public scrutiny. You should do this only with password schemes that can benefit from public exposure. If the whole trick of a password scheme is an ingenious idea that by publishing it reduces the password scheme's value, Keep It Secret.

Open source implementations of encryption algorithms, published research papers on algorithms and flaws thereof, and even this pattern language are examples of Lay It Open.

---

Previous pattern: Stay Current And Ahead

Next pattern: Keep It Secret

Contributors: Dirk Riehle

---

How much of the scheme should I make public? I think some of the patterns downstream in the language may be able to help the language user make choices about what should and shouldn't be laid out in the open. -- EugeneWallingford

# Keep It Secret

Synopsis: A publicly known password scheme does not provide as much protection as one that is kept secret.

---

Password schemes can get compromised by publishing them (as is done here). A determined cracker can use the knowledge about the scheme to develop an attack.

Therefore, if public exposure reduces the effectiveness of your password scheme, do not publish it. Or, if you do, use a secret variation of the password scheme.

Also, if you see your personal variation published somewhere else, change it.

---

Previous Pattern: Lay It Open

Next Pattern: Account Category

Contributors: Joe Bergin, Dirk Riehle

---

But as the number of passwords a person has and the complexity of the password schemes a person has increases, there is a great desire to record something somewhere. A link to the group of patterns beginning at Password Externalization, all of which address this force, might be nice. -- EugeneWallingford

With publishing I mean something different than Password Externalization. That information should still be kept secret! -- DirkRiehle

I think I see now. This pattern is about the "technology" of generating passwords, whereas Password Externalization is more about memory devices for a particular password. Is that right? -- EugeneWallingford

I wouldn't say "technology". It really is as simple as the advice to keep your secrets secret, under certain circumstances. It is the companion pattern to Lay It Open. Maybe it is too trivial a pattern. -- DirkRiehle

# Account Category

Synopsis: Align passwords with account categories.

---

A password like your dog's name may be easy to remember, but it is not very secure. However, it may be a viable choice for an account that has no security risk associated with it. Many read-only accounts on the Internet are of this nature, and there is no need to choose a complicated hard-to-remember password for them. Other accounts must be protected from misuse at (almost) all cost. For such accounts, a simple password won't do.

Therefore, create account categories based on the types of accounts you use, and put every account into exactly one category. Assign a password scheme to each account category, matching the value you associate with the accounts. Such a password scheme may be a single password or a password-creating algorithm.

---

Previous pattern: Keep It Secret

Next pattern: Typing Rhythm

Contributors: Dirk Riehle

# Typing Rhythm

Synopsis: For frequently used passwords, follow your typing rhythm.

---

Passwords can be a drag if you use them frequently but have to think hard before you remember them.

Therefore, choose frequently used passwords in such a way that they follow a typing rhythm that feels natural to you. This way, you can hammer them out fast.

In the case of low-risk accounts, the password may be a DictionaryWord. In the case of medium-risk accounts, you may think of a few keys on your keyboards as drums and tap out a rift that feels good, for example, 9ddd8eee7. In the case of high-risk accounts, the password may be an arbitrary letter/digit combination that follows specifics of your anatomy or typing patterns.

---

Previous pattern: Account Category

Next pattern: Singleton Password

Contributors: Dirk Riehle, Norm Kerth

---

It seems to me that having to think hard to remember a password is orthogonal to the typing rhythm of a password. Certainly, typing rhythm can help jog one's memory, but is a password long enough that one's beginning to type can help him remember the ending? TypingRhythm is important for other reasons, too. For example, when typing one's password in a room where others could conceivably watch, having a password that types quickly is good. A password that is out of the typer's natural rhythm can take longer and be more stilted, which gives observers more opportunity to Steal The Sign (that's a baseball metaphor). -- EugeneWallingford

I'm afraid you'll have to explain Steal The Sign to me. :-( --DirkRiehle

Sorry for the culture-specific reference... In baseball, the catcher signals the pitcher to indicate what kind of pitch to throw and to what location. If a batter can know that information, then he can be prepared for the pitch. If a baserunner can know that information, then he can make better decisions about trying to steal a base. The lore of baseball is replete with baserunners on 2nd base, or observers in the outfield, trying to Steal The Sign and thus gain an advantage. To combat this, teams often have multiple codes that they use to prevent information gathered yesterday from being useful to the other team today. The reason I mentioned this idea here is that another strategy is to camouflage their signals or take other measures to ensure that the observers don'd have an opportunity to detect the signal. Passwords that are out of the typer's natural rhythm give an observer more opportunity to Steal The Sign, and this is a force driving toward Typing Rhythm. -- EugeneWallingford

IMO memory by typing rhythm and memory by thinking hard are at different ends of a learning process for passwords. Things you type a lot go into the muscles, they become a rhythm rather than a 'word'. Things you don't type a lot stay 'words' that you have to think hard about to recall. -- SachaBrostoff

# Singleton Password

Synopsis: Use a sequence of regular words to form a larger password.

---

A common automated attack is to try every word in the dictionary. This takes about as long as trying every sequence of two characters.

Therefore, choose a password made of several words.

A password made of three words is about a good as one made of six letters, as long as it isn't a familiar phrase that shows up in some phrase book. For using words that don't go together, but are still easy to remember for you, use PrivateWordAssociation.

---

Previous pattern: Singleton Password

Next pattern: Unusual Variation

Contributors: Ward Cunningham

# Dictionary Word

Synopsis: Use a sequence of regular words to form a larger password.

---

A common automated attack is to try every word in the dictionary. This takes about as long as trying every sequence of two characters.

Therefore, choose a password made of several words.

A password made of three words is about a good as one made of six letters, as long as it isn't a familiar phrase that shows up in some phrase book. For using words that don't go together, but are still easy to remember for you, use PrivateWordAssociation.

---

Previous pattern: Singleton Password

Next pattern: Unusual Variation

Contributors: Ward Cunningham

# Unusual Variation

Synopsis: The more variations you use, the harder it is to crack.

---

Any of the techniques presented here can be compromised if used singly and as stated.

Therefore combine them and use variations of various sorts.

For example Dictionary Word can be varied by using unusual capitalization, punctuation, or spelling. Or, preferably, all three.

---

Previous pattern: Dictionary Word

Next pattern: Password Salt

Contributors: Joe Bergin

---

Note: Maybe this is two patterns, one for combinations and one for variations. -- JoeBergin

How similar is it to Password Salt? -- DirkRiehle

I think it is more general. -- JoeBergin

I agree that Unusual Variation is more general than Password Salt. Password Salt seems to be about mutation of characters as a device (though it does speak more generally of adding a special character to the password, too). I am reminded of genetic algorithms, which offer three forms of "reproduction": direct reproduction, in which a character is generalized or specialized; crossover, in which parts of two words are used to create a third; and mutation, in which one character spontaneously changes to some random other character. I can imagine using all three to generate passwords, especially from Dictionary Words. (Private Word Association is a degenerate form of crossover.) -- EugeneWallingford

# Password Salt

Synopsis: Make a password more complicated by adding simple mutations.

---

Limiting a brute force password search to alphanumeric characters makes the job of the password cracker too easy. The introduction of non-alphanumeric characters in a sequence of letters and numbers can consisiderably increase the search space for brute force attackers.

The addition of even a single non-numeric character to a password can prevent simple exhaustive dictionary or dictionary pair attacks from succeeding. Character substitition schemes, such as subsituting "!" for "i", or "@" for "a", can similarly complicate such strategies.

Therefore, add an easily remembered non-alphanumeric sequence to your most cherished password. Try to vary it so that if one is compromised, all your passwords are not.

---

Previous pattern: Unusual Variation

Next pattern: Password Algorithm

Contributors: Anonymous Contributor

# Password Algorithm

Synopsis: For infrequently used passwords, use a password-creating algorithm.

---

For a medium to high-risk Account Category, a single password isn't appropriate, because you might compromise all accounts in that category. On the other hand, if there are too many accounts in that category, you may not want to come up with an individual password for each of them, in particular if you use the accounts only infrequently.

Therefore, develop a password-creating algorithm for such a high-risk but infrequently used category.

For example, the account name or service provider may serve as the input to the algorithm, and a password unique to this account is the output of the algorithm.

Also, other elements of the context may seed a simple password-creating algorithm based on a personal category such as sibling initials and birth dates plus non-alphanumeric Password Salt. These can be easy for a particular individual to generate, but fairly difficult for an outsider to regenerate, without resorting to an intrusive search of personal information regarding the generators of said passwords.

---

Previous pattern: Password Salt

Next pattern: Codebook

Contributors: Dirk Riehle, Anonymous Contributor

# Codebook

Synopsis: Use a printed book as a source of passwords if you need to generate a lot of them.

---

If you need to generate a lot of passwords or pass phrases you can use a printed book. For example, if you want pass phrases, the next one you generate is the first few words of the next line of the current page of your book. If you keep a Master Account File you can remember the phrase just by knowing the index of the account in the master file.

You can, of course, use the printed book much more creatively than the simple example above. Once you think of a creative way you should probably Keep It Secret.

However, all your passwords can be compromised if the book/edition is known. It might be best to use an obscure book or rare edition. Also, don't forget that Project Gutenberg has lots of older books in electronic form. Don't use this in such a way that an attack can be automated via these texts. See http://promo.net/pg/

Your favorite book is probably a bad choice as it may be easily associated with you. So I won't use "One Hundred Years of Solitude," for example. A book you wrote is also a bad idea.

Known Uses: A classic spy technique is to carry a book and to use it to generate codes. The confederate has a copy of the same book for decoding.

---

Previous pattern: Password Algorithm

Next Pattern: Password Externalization

Contributors: Joe Bergin

# Password Externalization

Synopsis: Use visual or other helps that play to your individual capabilities to remind you of passwords.

---

Singleton passwords are frequently difficult to remember, because of their arbitrary nature. Stopping short of writing them down somewhere, you need a way to externalize them so that you can look them up.

Therefore, use your primary trait to encode a password in something that plays to your trait.

If you are a visual person, use something visual, like a tree, or a crossword puzzle in which you encode your password. If you are an auditory person, use the patterns you recognize in the Ode to Joy or something similar. If you are an olfactory person, I can?t help you, but you probably know best how to associate textual patterns with the smell of your beloved one.

For example, some banks gave customers credit-card-sized prints that featured a matrix of digits into which customers visualized their pin codes. Also, some people hide pin codes in their phone books as phone numbers.

---

Previous pattern: Codebook

Next pattern: Master Account File

Contributors: Dirk Riehle

# Master Account File

Synopsis: If you must, maintain a master account file, but no master password file.

---

At some point in time, your account categories and password schemes are likely to outgrow the reliability of your memory. Having to write down passwords may seem the consequence, but it has the risk that someone gets access to your master password file, and then you are really screwed.

Therefore, if you must externalize this critical body of information, write down your account categories without the passwords, and use some of the other patterns, like password externalization or typing rhythm to remind you of the passwords.

Depending on the severity of having your accounts exposed, you may not want to store the file electronically but only keep a paper copy.

---

Previous pattern: Password Externalization

Next pattern: Password Lock Box

Contributors: Dirk Riehle

# Password Lock Box

Synopsis: If you must, create a master password file, but protect it with your highest level of security.

---

If your life gets so complicated that Master Account File no longer works, you may need to capture all of the account-password information you have electronically. If you must do this, make sure that it is kept encrypted with the best algorithm and that the password to this one is in your highest level Account Category, and is never written down.

Known Uses: On the Macintosh, a program called the Keychain manages passwords. However, all your passwords are compromised if your keychain is. It should be autolocked after each use, but is not. It will, however, take a long pass phrase for its password.

Similarly, PGP keeps private keys electronically on your machine and uses them automatically, but hides them behind long pass phrases. It also gives you hints about how secure your pass phrase is when you create it, though I think it may use only the length to do so.

---

Previous Pattern: Master Account File

Next Pattern: Password Hint

Contributors: Joe Bergin

# Password Hint

Synopsis: Keep a hint that helps a user remember his or her password.

---

A hint is a message that helps a user remember a forgotten password. This does not improve security, but it does improve the practical use of passwords. The system should usually encourage users to use a hint that relies on information not many people would know. For example, "My first pet's name" may be a reasonable hint. A more common and thus less secure hint is, "My mother's maiden name."

You may want to use some security, including the use of another password, to make the hint available only to someone with a little information. For example, you might make hints available only to someone that know's a person's ID number.

---

Previous Pattern: Password Lock Box

Contributors: Steve Metsker

---

This pattern has some interesting memory-aid implications relative security. For example, I wouldn't want my password to **be** my mother's maiden name, because anyone could know that. But it seems that a Password Hint could serve as the initiation for a Private Word Association, and so can be part of how we remember a password and how we generate it. Using a Private Word Association that can't be remembered easily defeats the purpose. -- EugeneWallingford

I'm not sure about this pattern. Something like "mother's maiden name" is used for identification purposes if you call in when you have to inquire about your forgotten password. So it is like a simpler password to get back to your original password. -- DirkRiehle

Yes, I think that's so. That's why I think the hint mechanism should be implemented with some of the same care that the password is. This leads to something of an infinite regress, I suppose. -- EugeneWallingford

My mother's maiden name has another large problem. With the growth of internet genealogy, obtaining this information has become trivial. -- Nick Leaton