gnu-pw-mgr - derive a password from an id

For version , June 2018

Bruce Korb
bkorb@gnu.org

This manual is for gnu-pw-mgr version , updated June 2018

Copyright © 2013-2018 by Bruce Korb.

> Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, with no Front-Cover Texts and no Back-Cover Texts.

Table of Contents

This program is designed to make it easy to reconstruct difficult passwords when they are needed while limiting the risk of attack. The user of this program inputs a self-defined transformation of a web site URL and obtains the password and user name hint for that web site. You must, however, be able to remember this password id, or the password is lost forever.

The Wikipedia has an excellent article (https://en.wikipedia.org/wiki/Password_strength) on passwords in general and there is a paper published at Stanford (http://crypto.stanford.edu/PwdHash/pwdhash.pdf)* that describes a browser plug-in that is substantially similar to this program.

* Blake Ross; Collin Jackson, Nicholas Miyake, Dan Boneh and John C. Mitchell (2005). "Stronger Password Authentication Using Browser Extensions". Proceedings of the 14th Usenix Security Symposium. USENIX. pp. 17–32

1 Introduction to password management

This introductory chapter will superficially cover password management issues and describe how this program addresses them.

1.1 How evil-doers access your accounts

First and foremost, because people give them their credentials (user name and password). Not deliberately, of course. They leave them around or reply to a phishing scam or whatever. There's nothing providers of security assistance can do about it. That's the user's responsibility. Be careful out there. Keep your systems clean of spyware and watch for phishers.

The next most common method is for a site to get "hacked" and the crooks make off with password files. Hopefully, they've been hash encoded, but they are sometimes in the clear. If they are hashed, then the crackers will try to reverse the hash and see how far and wide they can use your credentials.

Other possibilities are telescopes, line taps, wireless sniffing and so on. Unless you are a secret agent working on national security matters, these possibilities are not terribly likely possibilities.

The purpose of this software is to render useless, limit the potential damage, or, at least, make it difficult to gain much use out of any information captured. And, also, make it convenient enough to use that it is actually used. A very secure password scheme that is a nuisance to use, won't be used, and is therefore not very useful.

1.2 How to keep evil-doers at bay

First and foremost, make sure you know which web site you are interacting with when you supply credentials. Do not blindly click an email that looks like one from Pay Pal or your bank. Go to your financial institutions via a bookmark or a well-established link.

Next, use different passwords at different web sites. Unless you restrict yourself to very few web sites, this means you must manage them somehow. Pieces of paper get lost. Password list files can wind up getting compromised. If that happens, your entire online world is now open. Encrypted password list files can get decrypted, yielding the same possibility.

Do not use either words or common transformations of words for passwords. Such techniques severly limit possibilities and constrained possibilities are searched more quickly.

Use long passwords. The longer they are, the more difficult (compute costly) they are to break.

1.3 How gnu-pw-mgr helps

Passwords must be long, not based on dictionary words, never repeated, and not recorded where they can be gotten at. You can't do it by memory.

This program addresses the recording problem by not recording passwords. They get re-computed every time, based on two separate factors each of which is unlikely to come into the hands of miscreants. The first factor is a series of one or more password "seeds" or "salts". You specify a tag for it and the seed itself is a block of text that contains at least 64 characters. The second factor is a transformation of the web site address. That transformation should be easy to remember, fairly easy to type, include odd capitalization, use multiple unusual punctuation characters, have a secret word or two and never, ever be written down.

The text, the URL transform and the tag get hashed together to construct the password. Since different web sites have different password requirements and allowances, the result is trimmed and tweaked until it meets the requirements. It is always possible that new requirements might pop up, and the password polishing code has been written to be extensible.

Using this program not only makes it simple to have different passwords for different web sites, it actually makes it inconvenient to use the same password. It does not support the same password, so you would have to remember the jumble of letters and numbers for any alternate web site. You won't do that.

`gnu-pw-mgr` works by storing the seed in a private configuration file and obtaining the password identifier either from the command line or by reading it from standard input. This configuration file must be secured from reading and writing by other users, but obtaining access will not reveal passwords. The key to this is the *password identifier*. It is the second factor in the authentication (password re-creation) that is never recorded.

The configuration file does not need to be super secret. What needs to be super secret is the transformation used for constructing password identifiers. That transform includes a prefix, a suffix, alternate capitalizations and a variety of word separators. For example, you could prefix every domain name with "access" and suffix it with "por-favor", then use an unusual spelling of the domain, perhaps "ExAmplE.moC". This yields a password id of "access/ExAmplE+moC=por-favor". You can remember that fairly easily. If a bad actor gets your seed file, they won't work out the transform any time soon.

On the other hand, if someone does happen to see you create the transform, it will still do no good, unless they also get the second factor: the seed file. This is true even if they also get one password. There is no way to derive the seed file from the password id and the resulting password. It is a one way hash function. It is not an encryption.

Every site has their own set of attributes that make for acceptable passwords, so the hash of the inputs must be modified. The hash of the password id by itself is used as a key to look up any previously established password constraints (see Section 2.3 [password options], page 10). These password attributes are length, character types required and/or prohibited from being in the password and some hint about your login name or id. That name need not be exactly your login name, just something that will remind you about which one you use for the site. It may be omitted, if you are sure you can remember.

These site specific options are then used to constrain the alphabet used to construct the password.

1.4 The answers to security questions

Many sites now add security questions that you must answer when you first set up your account. There are several problems with these:

1. The questions are often common, so if the answers become known from one site, the answers can be used at another.
2. Some answers can be researched.
3. Sometimes, you may select an answer that turns out to be difficult to remember or changes for you at some point.
4. If an answer requires two words, you are often out of luck. “Pick one.”

It’s a mess. `gnu-pw-mgr` supports a ‘`--confirm`’ option for answers to confirmation/security questions. Give that option a word or two from the question, and it will print out a 12 character sequence of alphabetic characters that are unique to the web site and unique for the option argument. For example, in the `gnu-pw-mgr` program’s `base.test` test, the confirmation option arguments `dog` and `pet` produce the strings `xkzrraogchyh` and `brrxsbesatfj`, respectively. These may be answers to the questions, ‘`what was your dog’s name`’ or ‘`what was your favorite pet`’, for example. These answers are valid only for the ‘`who`’ password id and the test’s seed string. With a different password id or seed, you would get a different answer.

NOTE: I have finally figured out that it is inconvenient to have the security question answers change when passwords change. Therefore, this option will, henceforth, print *two* answers. The first will change whenever the password changes. The second will only vary on the input password id and confirmation text.

1.5 Sharing a password with someone

Sometimes in a household or with a partnership it becomes necessary to have a common login to some web sites. To accommodate this and to not reveal to your partners how to login to the rest of your world, a new option has been added: `--shared`. Password seeds will be marked as either being “shared” or not and login ids will also be so marked. The emitted passwords for any login id will only be for those password seeds that match the shared/not-shared setting.

You are expected to transform a domain name into a password id using a method you would share with your partner and not use your personal transformation. To remind yourself that you need to use this alternate password id, you should put a reminder into the `--login-id` option for the usual domain transform.

FOR EXAMPLE:

Assume you wish to share your `nytimes.com` login. Let’s say your id transformation is to apply “private %s” to your domain names, yielding “private amazon.com” for your normal Amazon login. You should not reveal that to your partner. Instead, you want to use, “shared %s” yielding a password id of “shared nytimes.com”. More likely than not, you will forget. Therefore, do the following:

```
gnu-pw-mgr --tag first --text \
    'She sells sea shells [...] sea shore.'
gnu-pw-mgr --tag xxx --shared --text \
    'Peter Piper picked [...] did Peter Piper pick?'\

gnu-pw-mgr --log 'multi-user' --shared shared nytimes.com
gnu-pw-mgr --log "private vs. shared" private nytimes.com
```

now when you try the standard transform of `nytimes.com`, you get the reminder, “private vs. shared”. e.g.:

```
$ gnu-pw-mgr --status private nytimes.com
password id 'private nytimes.com':
  login-id   private vs. shared
$ gnu-pw-mgr --status shared nytimes.com
password id 'shared nytimes.com' (shared password):
  login-id   multi-user
$ gnu-pw-mgr  private nytimes.com
seed-tag     login id hint: private vs. shared   pw:
first        vpEzyiue8oZwb0Ov

$ gnu-pw-mgr shared nytimes.com
seed-tag     login id hint: multi-user   pw:
xxx          7VB1er/hzJOlydM1
$ cat ~/.local/gnupwmgr.cfg

<seed>
  <tag>xxx</tag><ver type=integer>1054726</ver><shared/>
  <text>Peter Piper picked [...] did Peter Piper pick?</text>
</seed>

<seed>
  <tag>first</tag><ver type=integer>1054726</ver>
  <text>She sells sea shells [...] sea shore.</text>
</seed>
<program per_pw_id>
<pwtag id="xWUK3...Pn+p">login-id  = 'multi-user'</pwtag>
<pwtag id="xWUK3...Pn+p">shared</pwtag>
<pwtag id="p5K9i...6tJL">login-id  = 'private vs. shared'</pwtag>
```

1.6 Keeping track of too many domains

I have been using this program for several years now. I have discovered that it is helpful to purge old clutter that I do not want to keep around any more. But I cannot because I do not know which entries in the configuration file are unused. There is now a new command line option:

```
--domain domain-name
```

Every time you use `--domain example.com`, a domain entry will be added or updated with the day count since 1970.

If you choose to use this, I must emphasize very strongly: *do not use a password id.* The names are stored in plain text. You are expected to use a transform to convert a domain into a password id. That transform should only be known by you and not be stored anywhere (outside your own brain).

2 Invoking gnu-pw-mgr

The password id should contain a fairly consistent permutation of the URL you are logging in to. "Fairly" because you may wish to vary your financial institutions differently than your newspaper, or you may need multiple credentials for the same domain. Either way, a password id is formed by surrounding the domain name with unlikely prefixes, suffixes and punctuations.

Only the passwords for one password id are ever printed. If the command line contains multiple operands (arguments after the options), then they are assembled into one password id with space characters separating the original operands. One password is printed for each seed stored in the password configuration file.

One password is printed for every configured seed value with a matching `--shared` option state. Seed values are added by specifying just the `--tag` and `--text` options, with or without the `--shared` option. When passwords are printed, the tag is also printed in plain text.

Passwords are changed by specifying the `-r` or `--rehash` option with a new numeric value. The day this happens will be noted in the password configuration file and printed in the password header.

Password ids are never stored anywhere.

Please be sure to read the "Warnings" section in the full documentation.

NOTE: the `--load-opts` option is supported by the option processing library. This program actually prohibits its usage. The password configuration database is normally found in a standard location. It may be overridden at invocation time by the `--config-file` option. Using `--load-opts` on the command line will lead to a conflict error.

Example usage can be seen in the example section below.

This chapter was generated by **AutoGen**, using the `agtexi-cmd` template and the option descriptions for the `gnu-pw-mgr` program. This software is released under the GNU General Public License, version 3 or later.

2.1 gnu-pw-mgr help/usage (`--help`)

This is the automatically generated usage text for gnu-pw-mgr.

The text printed is the same whether selected with the `help` option (`--help`) or the `more-help` option (`--more-help`). `more-help` will print the usage text by passing it through a pager program. `more-help` is disabled on platforms without a working `fork(2)` function. The `PAGER` environment variable is used to select the program, defaulting to `more`. Both will exit with a status code of 0.

```
gnu-pw-mgr - derive a password from an id - Ver. 2.3.2
Usage:  gnu-pw-mgr [ -<flag> [<val>] | --<name>[{=| }<val>] ]... [ <pw-id> ]

Options for adding and removing seeds in the configuration file.:

  Flg Arg Option-Name    Description
   -t Str tag            seed tag
                                - prohibits these options:
                                login-id
                                cclass
                                length
                                specials
                                no-header
                                use-pbkdf2
                                - may not be preset
   -s Str text           seed text
                                - requires the option 'tag'
                                - may not be preset
      no  shared         shared tag
                                - disabled as '--no-shared'
                                - may not be preset

Options for specifying password attributes.:

  Flg Arg Option-Name    Description
   -i Str login-id       a reminder of your login id
                                - may not be preset
   -l Num length         sets password length
                                - it must be in the range:
                                  4 to 128
                                - may not be preset
   -c Mbr cclass         password character class
                                - may not be preset
                                - is a set membership option
   -r Num rehash         rehash password with PKCS#5 PBKDF2
                                - prohibits the option 'use-pbkdf2'
                                - it must be in the range:
                                  1 to 100000
                                - may not be preset
      Num use-pbkdf2     rehash password with PKCS#5 PBKDF2
                                - disabled as ’--no-pbkdf2’
                                - enabled by default
                                - may not be preset
      Str specials       set alternate special characters
                                - may not be preset

Options for management and output format.:

  Flg Arg Option-Name    Description
   -H no  no-header      omit printing the password headers
                                - may not be preset
      Str select-chars   select only certain bytes of a password
                                - may not be preset
   -C Str confirm        confirmation question answers (see man page)
                                - may not be preset
   -S no  status         Show status of a password id
                                - may not be preset
   -d no  delete         Remove a password id entry
                                - may not be preset
      Str domain         a reminder of domains used for password id
                                - may not be preset
                                - may appear multiple times
      Str config-file    specify configuration file
                                - may not be preset

Options supported by the AutoOpts option library.:

  Flg Arg Option-Name    Description
   -v opt version        output version information and exit
   -h no  help           display extended usage information and exit
   -M no  more-help      extended usage information passed thru pager
      Str load-opts      load options from a config file
                                - disabled as ’--no-load-opts’
                                - may appear multiple times

Options are specified by doubled hyphens and their name or by a single
hyphen and the flag character.

The valid "cclass" option keywords are:
  alpha       upper       lower       digit       special     no-special
  no-alpha    no-triplets no-sequence pin         alnum       two-upper
  two-lower   two-digit   two-special
  or an integer mask with any of the lower 15 bits set
or you may use a numeric representation.  Preceding these with a ’!’
will clear the bits, specifying ’none’ will clear all bits, and ’all’
will set them all.  Multiple entries may be passed as an option
```

```
argument list.

The password id should contain a fairly consistent permutation of the URL
you are logging in to.  "Fairly" because you may wish to vary your
financial institutions differently than your newspaper, or you may need
multiple credentials for the same domain.  Either way, a password id is
formed by surrounding the domain name with unlikely prefixes, suffixes and
punctuations.

Only the passwords for one password id are ever printed.  If the command
line contains multiple operands (arguments after the options), then they
are assembled into one password id with space characters separating the
original operands.  One password is printed for each seed stored in the
password configuration file.

One password is printed for every configured seed value with a matching
'--shared' option state.  Seed values are added by specifying just the
'--tag' and '--text' options, with or without the '--shared' option.  When
passwords are printed, the tag is also printed in plain text.

Passwords are changed by specifying the '-r' or '--rehash' option with a
new numeric value.  The day this happens will be noted in the password
configuration file and printed in the password header.

Password ids are never stored anywhere.

Please be sure to read the "Warnings" section in the full documentation.

NOTE: the '--load-opts' option is supported by the option processing
library.  This program actually prohibits its usage.  The password
configuration database is normally found in a standard location.  It may be
overridden at invocation time by the '--config-file' option.  Using
'--load-opts' on the command line will lead to a conflict error.

Please send bug reports to:  <bkorb@gnu.org>
```

2.2 seed-options options

Options for adding and removing seeds in the configuration file.. The `--text` option or the `--tag` option (when by itself) tell the program to manage password "seeds" in its database (configuration file). Both options together add a new seed, and `--tag`, by itself on the command line, removes a seed.

seed option.

This is the “define a seed for a series of passwords” option. This option takes a hierarchy argument `SEED`. This option is **not** a command line option. It is also the only option that is directly processed from the config file.

The seed values consist of four named parts (sub-options):

‘`tag`’ These are displayed next to each displayed password to help identify them.

‘`text`’ This is not displayed, but is used for the SHA initial value. This may be arbitrarily long.

‘`ver`’ The version of `gnu-pw-mgr` used to initially store the seed. This is used to determine the password tweaking algorithm to use when the generated password does not meet the site criteria (see Section 2.3 [the password character class option], page 10). On rare occasions, new character class restrictions may cause a change in the algorithm used to tweak passwords. When this is done, the old algorithm is still used to tweak passwords from the older seeds.

‘`shared`’ The presence of this sub-option specifies that the seed is only to be used with password ids that are also marked as `--shared`. Without this sub-option, the seed is only used with password ids that are *not* marked as `--shared`.

The way to change a password is to specify the `rehash` count. It defaults to 10007. You can determine the current value with the `--status` option.

Specify only the `--tag` and `--text` (and maybe `--shared`) command line options and the program will initialize or insert a new value into the configuration file. Specify only the tag and no other command line arguments, and the associated seed entry will be removed. All passwords using that seed will become unavailable. You cannot remove the last seed.

tag option (-t).

This is the “seed tag” option. This option takes a string argument `TAG`.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.
- must not appear in combination with any of the following options: login-id, cclass, length, specials, no-header, pbkdf2.

The tag for a seed to be added to or removed from the config file. The use depends on whether or not there is a `--text` option.

text option (-s).

This is the “seed text” option. This option takes a string argument `TEXT`.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.
- must appear in combination with the following options: tag.

The text for a password seed to be added to the config file. This text cannot include the 7 character sequence `"</text>"`. There must always be at least one. Multiple text seeds will cause multiple passwords to be printed out.

This text must be at least 64 characters long. The expectation is you will write a sentence or two that you can easily remember, including any capitalization, punctuation and spacing. You should include some non-alphabetic, non-digit characters here and there to make a dictionary attack more difficult. But if you need to reconstruct this, you need to remember them.

If the text is shorter than 64 characters, it will be padded out. In such a case, you will need to save the configuration file some place secure or it will be extremely difficult to reconstruct it, should that become necessary.

The original expectation was that passwords would be updated on an occasional basis. Now that I have over 100 login credentials, it is clearly infeasible to go around and update them all. Instead, I have to decide which are important to update and use the `--rehash` option to change the rehash count. The date of the last rehash count change is recorded with the password id options.

shared option.

This is the "shared tag" option.

This option has some usage constraints. It:

- can be disabled with –no-shared.
- may not be preset with environment variables or configuration (rc/ini) files.

If this option is used on conjunction with the `text` option, that seed is marked as a shared password seed and derived passwords are only printed for password ids that have been marked as shared. When used in conjunction with a password id, then the password id will be marked as a shared. Passwords will only be printed for seeds and ids that have matching "shared" settings.

2.3 password-options options

Options for specifying password attributes.. The `--cclass`, `--length`, `--tag`, `--shared` and `--specials` options are stored in the configuration file. They are associated with a password ID via a clipped sha check sum of the id. They will be recalled the next time that id is used.

login-id option (-i).

This is the "a reminder of your login id" option. This option takes a string argument.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

It is sometimes difficult to remember your login name for a given site. Or even, perhaps, if you have ever set up an account on a particular site. By specifying this option, you will know both that you have set it up and you will have a reminder what your login name is. Avoid using your real login name.

Also, there are now some sites that send password credentials to a validation domain that is common among several domains. Since this application forces you to use different passwords for different domains and these domains force you to use the same password for different domains, this option solves the irresistable force and immovable object dilemma. For each of the dependent domains, specify this option that will remind you of the correct password id.

The `login-id` has no effect on the final password, so it may be specified or altered at any time.

length option (-l).

This is the "sets password length" option. This option takes a number argument.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

Some web sites are more restrictive. Some are more generous. Use of this option requires a `<pw-id>` operand.

Password lengths of 4 through 7 characters are limited to "pin" numbers. "pin" numbers are 4 or more digits. All other passwords must be at least 8 characters long. The default length is 16. Use at least 24, if you can.

cclass option (-c).

This is the "password character class" option. This option takes a set-member argument.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.
- This option takes a keyword as its argument list. Each entry turns on or off membership bits. These bits can be tested with bit tests against the option value macro (OPT_VALUE_CCLASS). The available keywords are:

```
alpha       upper       lower
digit       special     no-special
no-alpha    no-triplets no-sequence
pin         alnum       two-upper
two-lower   two-digit   two-special
```

This option augments or specifies which character classes either must or must not appear in the final password.

Some sites disallow special characters, other sites require them, and still others require them, but only certain ones. If disallowed, specify `no-special` and special characters will be replaced with digits. If `special` is specified specifically, then in the absence of a '+' or '/' character, one character will be replaced with a hyphen. Other characters may be substituted for these three special characters with the `--specials` option.

Explanations of the keywords:

'`upper`' There must be at least one upper case letter.

'`lower`' There must be at least one lower case letter. Both this and '`upper`' together require one of each.

'`alpha`' There must be at least one alphabetic character, either upper or lower If either '`upper`' or '`lower`' is specified, this attribute is a no-op.

‘`no-alpha`’
: Alphabetic characters are prohibited. This conflicts with ‘`upper`’, ‘`lower`’ and ‘`alpha`’.

‘`digit`’
: There must be at least one decimal digit character.

‘`no-triplets`’
: When three characters in a row are the same, the third is fiddled. Letters are changed to the next letter and `z` becomes `a`. Digits are handled similarly. Special characters are replaced with the third possible special character (`-`, unless modified with `--specials`). (Yes, there are a few such sites.)

‘`special`’
: The password must contain at least one ‘`special character`’ (a non-alphabetic, non-digit character).

‘`no-special`’
: The password must not contain any characters that are not alphabetic or decimal digits.

‘`no-sequence The password must not contain a consecutive sequence`’
: of three or more characters.

‘`pin`’
: The password is all digits, a Personal Identification Number. This is an abbreviation for `no-alpha + no-special + digit`.

‘`alnum`’
: This is an abbreviation for `alpha + digit`.

‘`two-*`’
: Two of a particular character class are required. Specifying this implies "at least one of" the specified type. Two upper case, lower case, punctuation (special) and digit characters may be specified this way. “two-alpha” is not supported.

rehash option (-r).

This is the “rehash password with pkcs#5 pbkdf2” option. This option takes a number argument.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.
- must not appear in combination with any of the following options: pbkdf2.

By default, passwords are created with the SHA256 hash of the "seed string", the password id and the tag text associated with the seed. If not disabled, the pbkdf2 funcion (with SHA1 as the HMAC function) is used to rehash the result a number of times. By default, this is done 10007 times. This can be over-ridden by specifying a different count. Changing the count will change the password and will mark the entry with the date of the most recent password change.

Please see RFC 2898 for a specification of the PBKDF2 (Password-Based Key Derivation Function version 2) function.

pbkdf2 option.

This is the “rehash password with pkcs#5 pbkdf2” option. This option takes a number argument.

This option has some usage constraints. It:

- can be disabled with –no-pbkdf2 and enabled with –use-pbkdf2.
- It is enabled by default.
- may not be preset with environment variables or configuration (rc/ini) files.

This is the deprecated spelling for the -r/–rehash option. This will be marked as not-for-command-line-use with the next release.

specials option.

This is the “set alternate special characters” option. This option takes a string argument.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

The password is a base64 encoding of a sha256 hash of various inputs. Base64 encoding uses '`+`' and '/' characters and when this program is required to have at least one special character in the result, it will replace one character with a hyphen (`-`).

However, some web sites require special characters and constrain them to be in a particular set that does not include these three: ‘`/+-`’. Therefore, specify this option with exactly three characters in the string argument. They will be used to replace the three characters above. The first two may be the same, but the third *must* be different from the first two. This option is accepted, but serves no purpose if `no-special` has been specified in the `--cclass` option.

2.4 formatting-options options

Options for management and output format..

no-header option (-H).

This is the “omit printing the password headers” option.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

By default, the output includes column headers. For confirmation output, the two values will have column labels, and for password output, it will contain any login hint and the date the last time the `--rehash` count was changed. (Password was changed.)

Suppressing it is intended for automated logins. The login name hint will not be provided, but the `tag` is printed.

select-chars option.

This is the “select only certain bytes of a password” option. This option takes a string argument.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

There exists at least one web site that asks you to enter just some of the password characters, like the second, tenth and sixteenth. With long, memorable resistant passwords, this can be difficult to do. For such web sites, provide this option with the string "2,10,16" as the option argument. The characters to select are space or comma separated values. The result cannot be longer than the original password.

confirm option (-C).

This is the "confirmation question answers (see man page)" option. This option takes a string argument.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

Some web sites use "confirmation questions" that, supposedly, only you know the answer to. Unfortunately, these are often times questions that can be researched by others or they can be questions that you have forgotten the answers to or may have multiple answers for. The net result is that you are locked out. This option makes it easy to get consistent answers to these questions and have these answers be different for every web site, just like your password.

Providing this option will cause the argument to be merged into the hash source (changing the resulting password). Exactly 12 letters will be extracted from the hash and converted to lower case. The string argument to this option should be the last word or two from the question, yielding an easy-to-remember way of obtaining a consistent answer to these inscrutable questions.

You will need to update your confirmation question answers when you update your password seed. However, since that can be highly inconvenient also, this option will print *TWO* results. The first will be dependent on the current password hash, the second will depend *only* on the confirmation question and password id. Consequently, the second one will be stable going forward. The first answer is now deprecated.

status option (-S).

This is the "show status of a password id" option.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

Show all the modified password attributes for a password id. If there are no special attributes, the word "default" is printed. No password id is invalid, but some may have all default values, consequently there is no special information kept about it.

Command line options will affect the output, but will not be stored for future use.

delete option (-d).

This is the "remove a password id entry" option.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

This will print out the attributes associated with a particular password id and remove them from the configuration file.

domain option.

This is the “a reminder of domains used for password id” option. This option takes a string argument `DOMAIN`.

This option has some usage constraints. It:

- may appear an unlimited number of times.
- may not be preset with environment variables or configuration (rc/ini) files.

If you create a lot of passwords, it is easy to forget which domains have an associated password. You do *not* want to specify a password id, merely note the domains for which you have a password id. With well over 100 passwords, I found I need to be able to know which need to be updated occasionally. This option will cause a separate text database to be updated with a domain name and an update date. With a single hyphen as the option argument, that database will be printed out in chronological order.

config-file option.

This is the “specify configuration file” option. This option takes a string argument `CONFIG-FILE`.

This option has some usage constraints. It:

- may not be preset with environment variables or configuration (rc/ini) files.

If you need an alternate location for storing your password seed files, use this option. It must be specified on the command line every time it is needed. You are responsible to ensure that the directory already exists. The file will be left read-only when gnu-pw-mgr exits. The containing directory permissions will not be checked or altered.

2.5 presetting/configuring gnu-pw-mgr

Any option that is not marked as *not presettable* may be preset by loading values from configuration ("rc" or "ini") files.

Configuration files may be in a wide variety of formats. The basic format is an option name followed by a value (argument) on the same line. Values may be separated from the option name with a colon, equal sign or simply white space. Values may be continued across multiple lines by escaping the newline with a backslash.

Multiple programs may also share the same initialization file. Common options are collected at the top, followed by program specific segments. The segments are separated by lines like:

```
[GNU-PW-MGR]
```

or by

```
<?program gnu-pw-mgr>
```

Do not mix these styles within one configuration file.

Compound values and carefully constructed string values may also be specified using XML syntax:

```
<option-name>
   <sub-opt>...&lt;...&gt;...</sub-opt>
```

```
        </option-name>
```

yielding an `option-name.sub-opt` string value of

```
        "...<...>..."
```

`AutoOpts` does not track suboptions. You simply note that it is a hierarchicly valued option. `AutoOpts` does provide a means for searching the associated name/value pair list (see: optionFindValue).

The command line options relating to configuration and/or usage help are:

version (-v)

Print the program version to standard out, optionally with licensing information, then exit 0. The optional argument specifies how much licensing detail to provide. The default is to print just the version. The licensing information may be selected with an option argument. Only the first letter of the argument is examined:

‘`version`’ Only print the version. This is the default.

‘`copyright`’
Name the copyright usage licensing terms.

‘`verbose`’ Print the full copyright usage licensing terms.

2.6 gnu-pw-mgr exit status

One of the following exit values will be returned:

‘`0 (EXIT_SUCCESS)`’
Successful program execution.

‘`1 (EXIT_INVALID)`’
the option/argument configuration is invalid

‘`2 (EXIT_NO_MEM)`’
insufficient memory

‘`3 (EXIT_BAD_USER)`’
no password entry for current user

‘`4 (EXIT_HOMELESS)`’
home directory could not be found

‘`5 (EXIT_PERM)`’
config file improperly protected

‘`6 (EXIT_NO_CONFIG)`’
config file missing

‘`7 (EXIT_BAD_CONFIG)`’
cannot update config file

‘`8 (EXIT_NO_SEED)`’
no seeds were specified in the config file

‘`9 (EXIT_BAD_SEED)`’
The seed value was invalid

‘`10 (EXIT_BAD_SELECT_CHARS)`’
the list of characters for the –select-chars option is bad

‘`11 (EXIT_NO_PWID)`’
no password id was specified

‘`16 (EXIT_CODING_ERROR)`’
There is a coding error that should be reported

‘`66 (EX_NOINPUT)`’
A specified configuration file could not be loaded.

‘`70 (EX_SOFTWARE)`’
libopts had an internal operational error. Please report it to autogen-users@lists.sourceforge.net. Thank you.

2.7 gnu-pw-mgr Examples

Before running the program to print a password, you must first initialize its database with at least one seed.

```
gnu-pw-mgr --tag "first-seed-tag" --text \
"This is only a ’test’.  Were it *real*,
you _would_ likely know?"
```

These two strings along with a password id are used to create a ‘`sha256`’ hash code password. So, now you are able to print a password.

```
gnu-pw-mgr --login-id "user-name" --length 32 \\
    --cclass=upper,lower,digit,special \\
    my example.com
```

In this example, the password id is the string "my example.com". The space character is inserted between the command line operands. The options are associated with this id via another ‘`sha256`’ sum of just the id. The "user-name" would typically be either your actual user name for the site, or something that could readily remind you of the login id. If omitted, just do not forget it. The length specifies the maximum length allowed for a password on the site. You will get a password of that length. The `--cclass` defines the allowed and/or required character class(es) for the passwords for the site.

With the above seed and invocation, you will see printed out exactly this:

```
seed-tag     login id hint: user-name   pw:
first-seed-tag iQiF1g5aLQ0JqFIUbR/svpTS+F/PCeoy
```

Henceforth typing just ‘`gnu-pw-mgr my example.com`’ will always yield this output. The options above are now associated with the password id via a hash code. The `gnu-pw-mgr` database (either `~/.local/gnupwmgr.cfg` or `~/.gnupwmgrrc`, but the former preferred) will now be this (hash code abbreviated):

```
<seed>
  <tag>first-seed-tag</tag>
  <text>This is only a ’test’.  Were it *real*,
you _would_ likely know?</text>
</seed>
<program per_pw_id>
```

```
<pwtag id="*HASH*">
  cclass = =alpha + upper + lower + digit + special
</pwtag>
<pwtag id="*HASH*">length = 32</pwtag>
<pwtag id="*HASH*">login-id = 'user-name'</pwtag>
```

2.8 gnu-pw-mgr Authors

Written by Bruce Korb.

2.9 gnu-pw-mgr Notes

This program specifies its own configuration file and disallows the use of any other. This file should be modified by running this program and not by editing it. The `--seed` and `--load-opts` options cannot be specified on the command line and the `--seed` option is only recognized in a configuration file.

Password ids should have some always-used prefix and/or suffix glued onto a domain name or some trivial permutation of the domain name. If you forget your password id, then the associated password is irretrievably lost. The prefix and suffix should be easily remembered. If you do not add a prefix or suffix and the configuration file becomes compromised, then you have lost the keys to all your passwords because it becomes trivial to guess password ids.

For example, always prepending '`_mine_`' to a domain would yield '`_mine_example.com`' for your password id at '`example.com`'. Password ids are not stored anywhere.

3 Invoking sort-pw-cfg

This program will sort (and merge) the per-domain password attributes. If there are duplicate entries, the last entry seen will survive. The result will be sorted by password id hash code and option name. Thus, any file containing more recent entries should appear last. If you have updated two different password ids in two different password configuration files without having merged them, you may have a merge problem. You will need to try to remember what you did.

The "header" portion of the config file (the seeds and the <program...> marker) are taken from the first config file listed and ignored in the remaining files.

Example usage can be seen in the example section below.

This chapter was generated by **AutoGen**, using the `agtexi-cmd` template and the option descriptions for the `sort-pw-cfg` program.

3.1 sort-pw-cfg help/usage (`--help`)

This is the automatically generated usage text for sort-pw-cfg.

The text printed is the same whether selected with the `help` option (`--help`) or the `more-help` option (`--more-help`). `more-help` will print the usage text by passing it through a pager program. `more-help` is disabled on platforms without a working `fork(2)` function.

The PAGER environment variable is used to select the program, defaulting to more. Both will exit with a status code of 0.

```
sort-pw-cfg - sort/merge password config file - Ver. 2.3.2
Usage:  sort-pw-cfg [ -<flag> [<val>] | --<name>[{=| }<val>] ]... \
                [ <cfg-file> ...]
  Flg Arg Option-Name    Description
   -o Fil output         send result to this file
   -d no  default        select default config file for first input file
   -v opt version        output version information and exit
   -h no  help           display extended usage information and exit
   -M no  more-help      extended usage information passed thru pager

Options are specified by doubled hyphens and their name or by a single
hyphen and the flag character.

If no arguments are provided, input arguments are read from stdin,
one per line; blank and '#'-prefixed lines are comments.
'stdin' may not be a terminal (tty).

This program will sort (and merge) the per-domain password attributes.  If
there are duplicate entries, the last entry seen will survive.  The result
will be sorted by password id hash code and option name.  Thus, any file
containing more recent entries should appear last.  If you have updated two
different password ids in two different password configuration files
without having merged them, you may have a merge problem.  You will need to
try to remember what you did.

The "header" portion of the config file (the seeds and the <program...>
marker) are taken from the first config file listed and ignored in the
remaining files.
```

3.2 output option (-o)

This is the “send result to this file” option. This option takes a file argument. Normally, the first named file is rewritten with the entries ordered by the hash code with duplicates removed. Use this option to redirect output to the named file.

3.3 default option (-d)

This is the “select default config file for first input file” option. Instead of starting with the first operand (or first file in the standard input file list), start processing password id's with the contents of the standard configuration file. The additional files will override or augment this file.

3.4 sort-pw-cfg exit status

One of the following exit values will be returned:

‘`0 (EXIT_SUCCESS)`’
: Successful program execution.

‘`1 (EXIT_INVALID)`’
: the option/argument configuration is invalid

‘`2 (EXIT_NO_MEM)`’
: insufficient memory

‘`3 (EXIT_BAD_USER)`’
: no password entry for current user

‘`4 (EXIT_HOMELESS)`’
: home directory could not be found

‘`5 (EXIT_PERM)`’
: config file improperly protected

‘`6 (EXIT_NO_CONFIG)`’
: config file missing

‘`7 (EXIT_BAD_CONFIG)`’
: cannot update config file

‘`8 (EXIT_NO_SEED)`’
: no seeds were specified in the config file

‘`9 (EXIT_BAD_SEED)`’
: The seed value was invalid

‘`10 (EXIT_BAD_SELECT_CHARS)`’
: the list of characters for the –select-chars option is bad

‘`11 (EXIT_NO_PWID)`’
: no password id was specified

‘`16 (EXIT_CODING_ERROR)`’
: There is a coding error that should be reported

3.5 sort-pw-cfg Authors

Written by Bruce Korb.

4 Warnings

Things to consider.

4.1 Cleanups that need doing

It is entirely possible that there are some web sites out there with password requirements that this program cannot (at present) necessarily comply with. There are some possible workarounds:

1. Request the addition of a new character classification flag. If the issue can be satisfied by fiddling the emitted password a little bit (with the `--use-pbkdf2` option), that would be faster and easier than implementing a new option.
2. Likely, something else, surely. Please send a bug report (preferably a patch :) so the issue can be fixed.

4.2 Shell history

It is imprudent to leave your invocations in your shell history. These are often stored away in your home directory, unless you do something to keep it out of your history. It should not be the end of the world because it is troublesome to also obtain the configuration file. Still, it is not wise to tempt fate.

If you use BASH for your shell,

```
HISTCONTROL=ignorespace:ignoredups
HISTIGNORE=gnu-pw-mgr *
unset HISTFILE
```

are your friends. Press the space bar before the command name, or specify that anything that looks like a "gnu-pw-mgr" command should be ignored or eliminate history entirely.

Also, if you put your password id's on the command line, they become part of the process history and can be found. If that is a conceivable problem, then you may prefer to not put it on the command line and then type it in in response to a prompt. Your password id will not be echoed back as you type it.

4.3 Best gnu-pw-mgr practices

Try out several password id transforms before changing all your passwords on all your sites. You may decide it is too hard or too easy and want to change it. However, once you have gone to the trouble of changing the passwords on a lot of sites, you won't be especially eager to do it again. So, play with it on one site you use a lot, change the password a lot as you change the transform and then make a good decision.

Once you need to or are required to change a password, simply specify a new "–use-pbkdf2" value for that password id. You may see its current value by specifying "–status".

When choosing your password id transform, use things that you can easily remember. Especially if some nonsense thing can be easily remembered. Separate the components with unusual things like multiple punctuation characters. Do odd things with the top level domain. cApitaliZe strangely. Use a slightly different transform for financial institutions. If someone gets ahold of your seed file, you want to hope that a dictionary attack will not be readily successful.

But lastly and most important: be sure you can remember your transform(s). If you forget, your password is gone. So choose what you can remember and be consistent.

4.4 Password reset arrangements

Some sites will allow you to set up password resets using alternate channels (i.e. not your primary email address). Take advantage of this whenever possible. If someone gains access to your email, you don't want them to reset all your passwords, intercept the restore access emails and, thus, gain access to all your password protected accounts.

Appendix A GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.
https://fsf.org/

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

0. PREAMBLE

   The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

   This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

   We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

   This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

   A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

   A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

   You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

   You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

   If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

   If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

   If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

   It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

   A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

   If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

   Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

   If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

   You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

   However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

   Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

    The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `https://www.gnu.org/copyleft/`.

    Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

    "Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

    "CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

    "Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

    An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

    The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C)  year  your name.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts.  A copy of the license is included in the section entitled ``GNU
Free Documentation License''.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with. . . Texts." line with this:

```
with the Invariant Sections being list their titles, with
the Front-Cover Texts being list, and with the Back-Cover Texts
being list.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.