Installation npasswd

Password Enforcer

19th of October 2000

Document name:	Installation npasswd
Version:	V 1.0
Author:	Ivan Buetler, Compass Security AG
	ivan.buetler@csnc.ch
	http://www.csnc.ch/
References:	npasswd reference
Date of delivery:	19th of October 2000
Document state:	PUBLIC

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

CONTENT

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1 Installation

1.1 Introduction

Npasswd is a replacement for the passwd command for UNIX. It subjects user passwords to stringent guessability checks to decrease the chance of users choosing vulnerable passwords. It addresses other deficiencies found of standard password change programs. Npasswd is designed to replace the programs passwd, chfn and chsh.

Npasswd should work under most versions of UNIX and UNIX-like operating systems. It does not replicate every feature of every password program on every UNIX platform. If the installer chooses to replace the system programs with npasswd, they will be preserved and used to perform the functions that npasswd cannot do.

Many UNIX platforms use shadow passwords, which makes it harder for a bad guy to obtain encrypted passwords. But there are still plenty of systems which have the encrypted passwords available for all the world to see.

Having shadow passwords in and of itself greatly reduces vulnerability to password crackers. But that protection is a function of the UNIX file system. If you use unsecure NIS or a misconfigured NIS+, you can still give away your passwords.

Combining intelligent password checking with a shadow database provides the best protection short of one-time use passwords or challenge/response smart card systems.

Configuring npasswd requires some thought on the part of the administrator. It's not a "plug and play" process. There are configuration options to select, and there is policy in the code that may not meet your needs.

1.2 Version control

Version	Author	Description	Filename
1.0	Ivan Buetler ivan.buetler@csnc.ch	Initial version saved on http://www.csnc.ch/download/	Installation-npasswd-V1.0.pdf

[Ivan] If you feel like having something you would like to see in this document, pls. Let me know. I will leave the version control chapter in the future. So everybody can see who did what on this document.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.3 System requirements

To build and install npasswd, you need...

- An ANSI compliant C compliation system. The GNU C compiler (gcc) is fine.
- The make utility. GNU make is fine.
- A modern Bourne shell which understands functions. The Korn shell may not work with the support and maintenance scripts.

1.4 About package

The npasswd package produces the following components which share infrastructure and code:

- The npasswd program which changes passwords, login shells and finger information.
- The checkpassword program which does password checking.
- The checkpassword library which can be linked into other applications.

1.5 Installing

Installing

Invoke make install in the top-level build directory.

- The install will create any needed directories.
- Dictionary hash files will be built. The word list distribution must have been unpacked into the **dict directory** first.
- Executables and ancillary files are placed in the install directory.
- If replace system programs was selected, the system password change utilities found by configure will be saved and replaced with copies or links to the npasswd binary.

De-Installing

Make deinstall within the source tree

1.6 Configuring npasswd

Configure your password policy in /usr/lib/passwd/passwd.conf

Read the HTML documentation in order to understand the configuration file. At the beginning of passwd.conf, you can find some outcommented hints how to configure. The default settings are describen in the HTML documentation within the docs directory.

passwd.Message	/usr/lib/passwd/passwd.motd
passwd.History age	100
passwd.History depth	10
passwd.History database	file /usr/lib/passwd
passwd.MinPassword	8

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

2 Appendix

Npasswd Reference Manual

Introduction to the configuration file

The configuration file is **@NPASSWD-HOME@/passwd.conf**. This location can changed only by running *Configure* and rebuilding.
Npasswd will abort if the configuration file has syntax errors, or or fails any of the following security requirements:

- It must be owned by the uid that npasswd runs with (usually root).
- It must be a regular file (symlinks are **not** acceptable).
- It **cannot** be world writeable.

The syntax of a configuration file can be checked with the **-XC** option, which disables the security checks.

Syntax of the configuration file

Blank lines and lines starting with "**#**" are ignored.
Npasswd performs the functions of three standard UNIX utilities: **passwd**, **chfn** and **chsh**. Each of these **sub-programs** have their configuration directives.

Configuration directive syntax			
sub-program	**option**		**value**
One of **passwd**, **chfn**, **chsh**, or empty. A non-empty sub-program must be followed by a period (".")	Sub-program option (see below)	One or more whitespace characters	Value for *option* (see below)
Value types			
number	May be decimal (with an optional leading minus sign), octal (format **0NNN**) or hex (format **0xNNNN**)		

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

path	UNIX pathname
boolean	One of the strings "**1**", "**true" "yes**" or "**on**". Any other value is interpreted as **false**
string	Strings can optionally be enclosed in single (') or double (") quotes Non-printable ASCII characters can be specified thusly: • **^<**caret**char**" e.g. **^X** for control-x • "**\<**backslash**char**" for C special characters (\b \f \h \n \r \t \\) • "\0**NNN**" where **NNN** is the character value in octal • "\0x**NN**" where **NN** is the character value in hex

Summary of configuration directives

Npasswd configuration directives Directive and options are case-insensitive		
Directive	**Value Type**	**Description**
Directives applicable to all sub-programs		
MatchTries	number	Chances to give user to correctly enter a password.
MatchWait	number	Delay after the user enters an incorrect password.
PasswdTolerance	number	Tolerance between old and new passwd files.
ShadowTolerance	number	Tolerance between old and new shadow files.
Directives for sub-program "passwd"		
passwd.AlphaOnly	boolean	Allow alpha-only passwords
passwd.CharClasses	number	Set number of required character classes.
passwd.Dictionaries	path	Add to dictionary lookup path.
passwd.DisallowedChars	string	Set which characters are not allowed in passwords.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

passwd.Help	path	Help file for passwd.
passwd.History	See below	Configure history mechanism.
passwd.LengthWarn	boolean	Warn about passwords over maximum length.
passwd.MaxPassword	number	Maximum effective password length.
passwd.MaxRepeat	number	How many adjacent repeat characters allowed.
passwd.Message	path	Message of the day.
passwd.MinPassword	number	Minimum password length.
passwd.PasswordChecks	string	Select password checks.
passwd.PrintableOnly	boolean	Deny non-printable characters.
passwd.SingleCase	boolean	Allow single-case passwords.
passwd.WhiteSpace	boolean	Allow whitespace characters in passwords.
Directives for sub-program "chfn"		
chfn.Help	path	Help file for chfn.
chfn.Message	path	Message of the day.
Directives for sub-program "chsh"		
chsh.Help	path	Help file for chsh.
chsh.Message	path	Message of the day.
chsh.Shells	path	List of blessed shells.

Directives applicable to all sub-programs

MatchTries

Directive	Type	Default value
MatchTries	number	3

How many chances to give the user to correctly enter a password (old or new).

MatchWait

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Directive	Type	Default value
MatchWait	number	2

How many seconds to wait after the user enters an incorrect password.

PasswdTolerance

Usage	Type	Default value
PasswdTolerance	number	128

After the passwd file changes are done, the size of the new file is compared to the size of the old file, to guard against data loss due to disk or file system error. **PasswdTolerance** sets how many bytes the new password file can be **shorter** than the original. In order to accommodate changes to the finger information, the default for this tolerance is generous.

ShadowTolerance

Usage	Type	Default value
ShadowTolerance	number	32

After shadow changes are made, the size of the new shadow file is compared to the size of the old shadow file, to guard against data loss due to disk or file system error. **ShadowTolerance** sets how many bytes the new shadow file can be **shorter** than the original. This setting is much smaller than **PasswdTolerance**.

Directives for sub-program "passwd"

See the **Npasswd Administration Guide**.

---

passwd.AlphaOnly

Directive	Type	Default value
passwd.AlphaOnly	boolean	true

Controls whether alpha-only passwords will be accepted. If this option is set, the requirement for non-alpha characters in a passwords is dismissed. Other character diversity requirements remain in effect.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

passwd.CharClasses

Directive	Type	Default value
passwd.CharClasses	number	1

Sets how many classes of characters are required.
The character classes are:

- Upper case alpha.
- Lower case alpha.
- Digits.
- Whitespace.
- Punctuation.
- Control characters.
  The higher the class setting, the more diverse mixture of characters required.

passwd.Dictionaries

Usage	Type	Default value
passwd.Dictionaries	path ... path	@NPASSWD-DICT@

Passwd.Dictionaries specifies directories containing password check dictionaries. Each directory is scanned for hashed dictionary files. Multiple directories can be specified either in one directive, or by multiple directives.
It is a fatal error if any of the following are encountered:

- A directory which cannot be scanned.
- Missing dictionary hash files.
- A dictionary hash file which is not a regular file (symlinks are acceptable), or is world-writable.

passwd.DisallowedChars

Directive	Type	Default value
passwd.DisallowedChars	string	ctrl-c ctrl-s ctrl-q ctrl-d ctrl-h ctrl-j ctrl-m ctrl-o ctrl-r ctrl-y ctrl-z ctrl-] ESC ctrl-\ DEL

Sets the list of characters (usually non-printable) not allowed in passwords. The default list includes the typical terminal special characters. To supplement the list, put a plus sign as the first character of the string.
If you allow non-printable characters in passwords (the default), it would be wise to check your system and add any terminal special characters not in the standard list.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

passwd.Help

Directive	Type	Default value
passwd.Help	path	@NPASSWD-HOME@/passwd.help

This file is presented if the user enters "?" in response to the new password prompt.

passwd.History

Npasswd can maintain a history of passwords to discourage frequent reuse. See the history section of **Npasswd Administration Guide**.

Directive	Type	Default value	Description
Age	number	180 (days)	Use only passwords younger than N days.
Depth	number	2	Use only the most recent N **old** passwords.
Database	See below	dbm @NPASSWD-HIST@	Select password history database method and location
	none	Password history is disabled	
	file /path/to/file	Store history in file /path/to/file.	
	dbm /path/to/file	Store history in DBM database in /path/to/file.	

passwd.LengthWarn

Directive	Type	Default value
passwd.LengthWarn	boolean	false

Controls whether a warning message is issued for new passwords longer than **MaxPassword**. This warning is to inform the user that the excess characters are not effective. The default is to suppress this message.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

passwd.MaxPassword

Usage	Type	Default value
passwd.MaxPassword	number	8*

Sets the maximum effective length for passwords. This reflects a limitation of the standard *crypt*(3), which encrypts only the initial **8** characters of the plaintext. On Ultrix and Digital UNIX (aka OSF/1) with enhanced security, this limit is **16**.
It is **not** an error for a password to be longer than the maximum, but the password checker can be configured to issue a warning. See **passwd.LengthWarn**.

passwd.MaxRepeat

Directive	Type	Default value
passwd.MaxRepeat	number	3

Controls how many adjacent repeated characters are allowed in passwords.

passwd.Message

Directive	Type	Default value
passwd.Message	path	@NPASSWD-HOME@/passwd.motd

This file contains the "message of the day" for passwd.

passwd.MinPassword

Usage	Type	Default value
passwd.MinPassword	number	6

Sets the minimum acceptable password length. Passwords shorter than six characters (the default) are very vulnerable to guessing attacks.

passwd.PasswordChecks

Directive	Type	Default value
passwd.PasswordChecks	string	lexical passwd local history dictionary

Specifies the order of password checks. See **Npasswd Administration Guide**.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

passwd.PrintableOnly

Directive	Type	Default value
passwd.PrintableOnly	boolean	false

Controls whether non-printable ASCII characters are allowed in passwords. Character printability is determined by using *isprint*(3). If this is set, passwords which contain non-printable characters will be rejected. Other character diversity requirements remain in effect.

passwd.SingleCase

Directive	Type	Default value
passwd.SingleCase	boolean	true

Controls whether single-case passwords are accepted. Character case is determined by using *isupper*(3) and *islower*(3). If this option is set the mixed-case requirement is dismissed. Other character diversity requirements remain in effect.

passwd.WhiteSpace

Directive	Type	Default value
passwd.WhiteSpace	boolean	true

Controls whether whitespace characters are allowed in passwords. *Isspace*(3) is used to determine if a character is whitespace.

Directives for sub-program "chfn"

---

chfn.Help

Directive	Type	Default value
chfn.Help	path	@NPASSWD-HOME@/chfn.help

The help file is presented to the user in response to "?" input.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

chfn.Message

Directive	Type	Default value
chfn.Message	path	@NPASSWD-HOME@/chfn.motd

The message of the day file for *chfn*.

Directives for sub-program "chsh"

chsh.Help

Directive	Type	Default value
chsh.Help	path	@NPASSWD-HOME@/chsh.help

Help file for chsh. The help file is presented to the user in response to "?" input.

chsh.Message

Directive	Type	Default value
chsh.Message	path	@NPASSWD-HOME@/chsh.motd

The message of the day file for chsh.

chsh.Shells

Directive	Type	Default value
chsh.Shells	path	/etc/shells

The list of blessed shells that users can select. If *getusershell*(3) is available, this directive is ignored.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Command line options

The main command line options of npasswd control the platform-independent features.

Some operating-system specific options may also be supported (e.g. SunOS 4, SunOS 5 and HP-UX). Others may be deferred to the vendor passwd program (usually preserved during the initial installation).

Refer to the manual page for the full list of supported options.

Command line options Multiple -X options may be given	
-Xc	**Read the configuration file, output settings and exit with 0 status.**
-XC*config-file*	**Check syntax of config-file and terminate. Exit status is 0 if file was ok, 1 if not. This option disables configuration file security checks.**
-XD*debug-level*	**Set debug output level.**
	Debug levels
	None.
	Mild verbosity.
	Trace user lookup.
	Trace user updating.
	Trace configuration processing.
	Trace password checking.
	More detailed tracing.
	All debugging.
-XF	**Suppress new password checking. This option is restricted to root and should be used very sparingly.**
-XI	**Read passwords from standard input instead of */dev/tty***

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

	This option is restricted to root.
-XV	Print version and patch level identification.
-Xf	Perform the "chfn" (change finger name) function.
-Xs	Perform the "chsh" (change login shell) function.

Document id @(#) Reference.html 1.12
Version 1.12
Last modified 10/14/98

Clyde Hoover
Academic Computing Services and Instructional Technology Services
The University of Texas at Austin