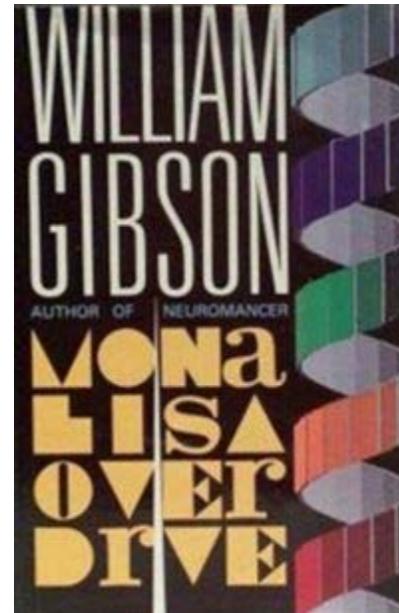


Password Management Ideas

Joel Anderson
5/10/2007

Where were you on the night of Wednesday, November 2, 1988?

I was driving to Odegaard's Bookstore in Minneapolis to get an autographed copy of this book:



... but, then – I wasn't a sysadmin.

If you were a sysadmin, you'd probably remember that the ***OTHER*** thing happening that night was Robert Morris's "Worm" spreading across the Internet. Taking advantage of flaws in sendmail and fingerd, the Worm spread by managing to crack many, many passwords.

The Internet Worm tried to crack passwords by working through a whole series of word lists. First, it built a customized dictionary of words containing the user name, the person's name (both taken from the Unix password file), and five permutations of them. If those failed, it used an internal dictionary of 432 common, Internet-oriented jargon words. If those failed, it used the Unix on-line dictionary of 24,474 words. The worm also checked for the "null" password. Some sites reported as many as 50% of their passwords were successfully cracked using this strategy.

<http://www.smat.us/sanity/pwdilemma.html>

This is one of the reasons why having a good password *matters*.

Define ***GOOD***.

“A good password is one that cannot be easily guessed.”

(Bearing in mind that “guessing” may involve high powered computer attacks. see Password Attack Discussion & Benchmarks by Alan Amesbury, <http://www1.umn.edu/oit/security/passwordattackdiscussion.html>)

In *Password Memorability and Security: Empirical Results* the authors did an experiment that tested password creation, strength and retention with three groups of students.

1. Naïve password choices (control)
2. Totally random choice
3. “Mnemonic phrase” password

(they also compared their subjects to a random sample of student accounts.)

This study

confirmed

- users have difficulty remembering random passwords
- passwords based on mnemonic phrases are harder to guess than naïvely selected passwords.

http://homepages.cs.ncl.ac.uk/jeff.yan/jyan_ieee_pwd.pdf

debunked

- random passwords are better than passwords based on mnemonic phrases. *In fact, each appeared to be as strong as the other.*
- passwords based on mnemonic phrases are harder to remember than naively selected passwords. *In fact, each type is as easy to remember as the other.*

And unfortunately, it debunked

- *we can significantly improve security by educating users to select random or mnemonic passwords*

In fact, **both** types of passwords suffered from a noncompliance rate of about 10 percent (including too-short passwords and passwords chosen contrary to the instructions). Although this is better than the approximately 35 percent of users who choose bad passwords with only cursory instruction, it's not a huge improvement*. The attacker might have to work three times harder, but without password policy enforcement mechanisms, we can't make the attacker work a thousand times harder.

** This is why it is good the internet and Enterprise passwords are subject to complexity requirements.*

Results of password attacks, by test group.

GROUP	PASSWORDS CRACKED USING FIRST THREE ATTACKS		PASSWORDS CRACKED USING BRUTE-FORCE ATTACKS
	NUMBER	PERCENT OF TOTAL	
Control group	30	32	3
Random password group	8	8	3
Pass phrase group	6	6	3
Comparison sample	33	33	2

Responses to the email memorability survey.

GROUP	RESPONSES	DIFFICULTY LEVEL (1-5)	WEEKS
Control group	80	1.52	0.7
Random password group	71	3.15	4.8
Pass phrase group	78	1.67	0.6

results from Jeff Yan, et al

Create a strong, memorable password in 6 steps

Use these steps to develop a strong password:

1. Think of a sentence that you can remember. This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as "My son Aiden is three years old."
2. Check if the computer or online system supports the pass phrase directly. If you can use a pass phrase (with spaces between characters) on your computer or online system, do so.
3. If the computer or online system does not support pass phrases, convert it to a password. Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".
4. Add complexity by mixing uppercase and lowercase letters and numbers. ... This might yield a password like "MsAy3yo".
5. Finally, substitute some special characters. You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i\$ 3 yeeR\$ old" or a password (using the first letter of each word) "M\$8ni3y0".
6. Test your password with a password checker.

<http://www.microsoft.com/athome/security/privacy/password.msp>

Offline test (requires *javascript*) :

Quick Links ▾ | Home | Worldwide

Search Microsoft.com for:

Microsoft

Security At Home
What's New
Latest Security Updates
Download Security Products
Protect Your Computer
Protect Yourself
Protect Your Family
Resources ▶
Worldwide Sites

[Security At Home](#) > [Personal Information](#)

Password checker

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

Test the strength of your passwords: Enter a password in the text box to have Password Checker help determine its strength as you type.

Password:

Strength: **Strong**

Related Links

- [Strong passwords: How to create and use them](#)
- [Help safeguard your personal information online](#)
- [Safer shopping online](#)

http://www.microsoft.com/athome/security/privacy/password_checker.msp

[X](#)

Online (php based) test:

SecurityStats.Com Password Strength Meter - Mozilla Firefox

File Edit View Go Bookmarks Tools Help del.icio.us

http://www.securitystats.com/tools/password.php

  **HANetworks.com**
7:26pm up 291 days, 1:41 1 users, load averages: 0.00, 0.00, 0.00

Your Portal to Statistical Security Data.™

Statistics

- Arrests & Convictions
- General InfoSec
- Security Spending
- Web Defacements
- Viruses
- Alarming News
- Reports and Papers
- Become a Stat!
- Search
- Home

Awareness Tools

- Tools Main
- Password Strength Meter
- Dictionary-Based Hash Cracker
- Cisco Hash Decoder
- Generic Hash Calculator
- HTTP Basic Auth Decoder
- Searchable Port and Protocol Index

Password Security

A good password is one that cannot be easily guessed.

Enter a password, click submit, then we'll score it against best practices!

Congratulations! You've supplied a sample password that is difficult to guess and hard to crack. It is recommended that you use passwords of this type.



Weak Password **Strong Password**

How scoring works: Your password will be checked for complexity against the guidelines below (See Suggestions). In addition, your password will also be checked against a hacking dictionary containing commonly used passwords and keystroke combinations.

<http://www.securitystats.com/tools/password.php>

NOTE

This online password-tester *DOES* introduce risk.

You should **NOT** use it for testing REAL passwords, but use it to *test* password complexity of sample passwords, and then use the results to gauge how complex your real passwords are.

Using this page means that the people running the password-test application will be given clues about password choice strategies within your network.

ONCE you have the password, now what?

- Memorize it!

<http://en.wikipedia.org/wiki/Mnemonic>

- Write it down!

http://www.schneier.com/blog/archives/2005/06/write_down_your.html

- Use a tool!

Tool tips

What should you look for in a password keeper?

- **Based on strong cryptography**

Does it securely store your information?

- **Open Source**

Benefit from active development community; no secrets, no snake oil

- **Portable**

Can you use it easily on more than one computer? Can it run from a flash drive?

Three tools for Password Keeping

- Password Safe (and friends)
- Truecrypt
- Locknote

Password Safe - <http://passwordsafe.sourceforge.net/>



[Secure your passwords now!](#)

[\[click here for latest version\]](#)

[Latest news](#)

[Non-English versions](#)

[Discussion forum](#)

[Project summary page](#)

[History](#)

[Related projects \(other platforms\)](#)

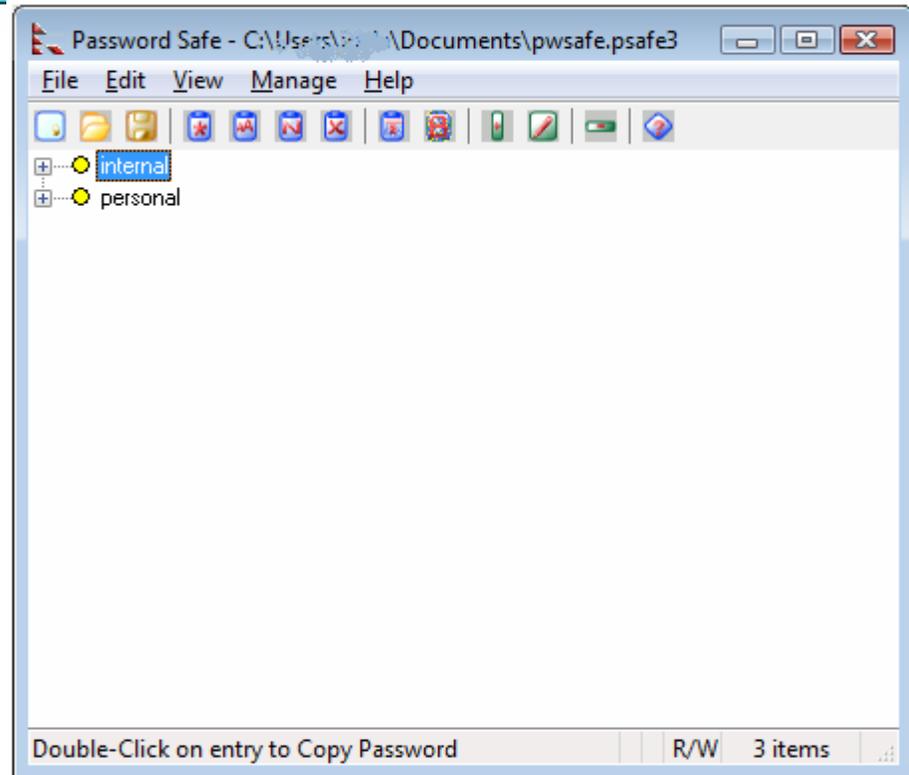
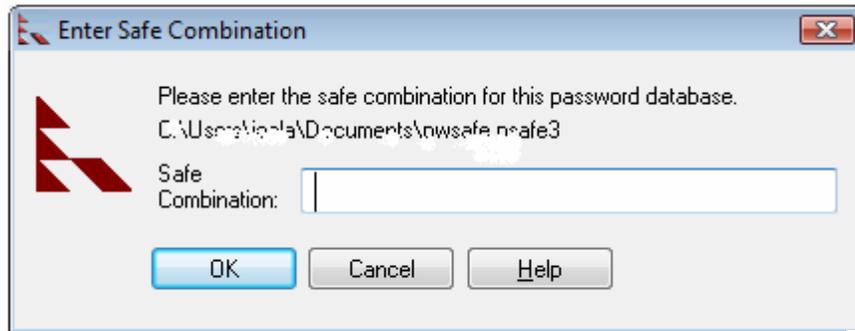
[Links](#)

Some testimonials from users:

- *I've tried many others, but I love the security & convenience of PasswordSafe*
- *I cackle with glee every time I use autotype :) We couldn't function without PasswordSafe!*
- *This software has become infused in my daily life. Nice piece of work!*
- *Great program, something I have been looking for and needing for a long time.*
- *This is a fabulous product that make remembering passwords so much easier.*
- [More...](#)

Password access

To multiple
accounts:



Multiple useful features

Add Entry [X]

To add a new entry, simply fill in the fields below. At least a title and a password are required. If you have set a default username, it will appear in the username field.

Group:

Title:

Username:

Password:

Confirm Password:

Notes:

Random Password

Override Policy

URL:

Autotype:

Advanced

Password expires on: Never

Keep last passwords

Options [X]

Password History Security System

Backups Display Misc. Password Policy

Random password generation rules

Default password length:

Use lowercase letters

Use UPPERCASE letters

Use digits

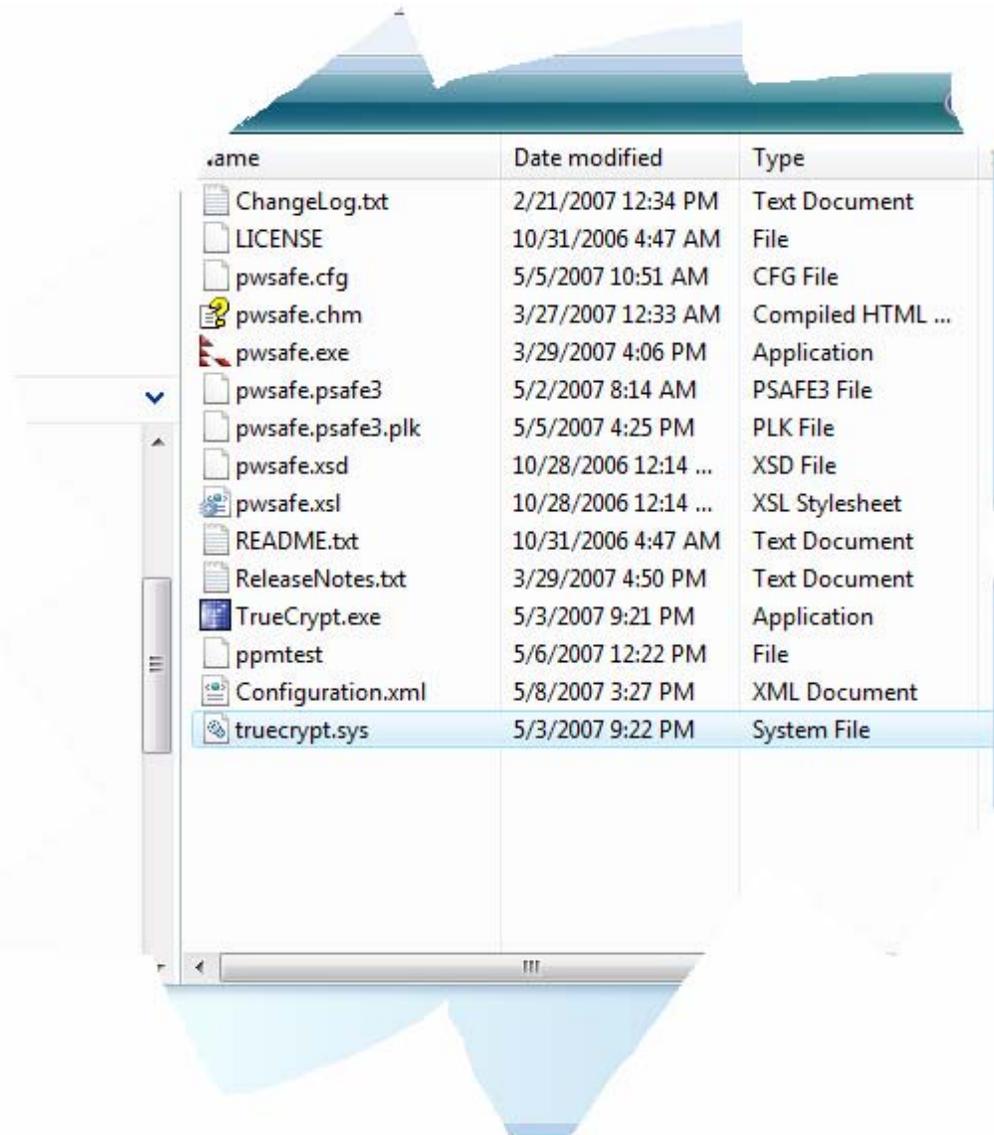
Use symbols (i.e., %, \$, etc.)

Use only easy-to-read characters (i.e., no 'l', '1', etc.)

Or

Use hexadecimal digits only (0-9,a-f)

Easy to install on a USB drive:



Other Developments

Pwsafe – command line version for multiple OS's

```
pwsafe password database

pwsafe is a unix commandline program that manages encrypted password databases.

Features:

  ♦ Pure command-line operation if desired (good for remote access over ssh)
  ♦ or can interact with X11 selection & clipboard.
  ♦ Portable, endianness-clean, misaligned-access-free C++. Compiles cleanly on linux, *bsd, macos x, solaris.
  ♦ Compatible with CounterPane's PasswordSafe Win32 program versions 2.x and 1.x.
  ♦ Funny comments included in source code.

Here are some screen shots, even though it is a CLI program.

Releases/Download

0.2.0
```

Pwsafe - <http://nsd.dyndns.org/pwsafe/>

Password Gorilla

A cross-platform Password Manager

Now [Available](#) for Microsoft Windows, Mac OS X, Linux, Solaris, *BSD, etc.

Free, Open Source Software!

Version 1.4



Password Gorilla - <http://www.fpx.de/fp/Software/Gorilla/>

TrueCrypt

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

[Home](#) [Documentation](#) [Downloads](#) [News](#) [Future](#) [History](#) [Screenshots](#) [Donations](#) [FAQ](#) [Forum](#) [Contact](#)

TrueCrypt

Free open-source disk encryption software for Windows Vista/XP/2000 and Linux

Hosted on:



News

• 2007-05-03
TrueCrypt 4.3a
Released

• 2007-03-19
TrueCrypt 4.3
Released

• 2006-10-06
Donations via PayPal
Accepted Now

[[News Archive](#)]

Main Features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- **Encrypts an entire hard disk partition** or a **storage device** such as USB flash drive.
- Encryption is automatic, real-time (on-the-fly) and transparent.
- Provides two levels of **plausible deniability**, in case an adversary forces you to reveal the password:
 - 1) **Hidden volume** (steganography - more information may be found [here](#)).
 - 2) No TrueCrypt volume can be identified (volumes cannot be distinguished from random data).
- Encryption algorithms: AES-256, Serpent, and Twofish. Mode of operation: LRW.

Further information regarding features of the software may be found in the [documentation](#).

[What is new in TrueCrypt 4.3a](#) (released May 3, 2007)

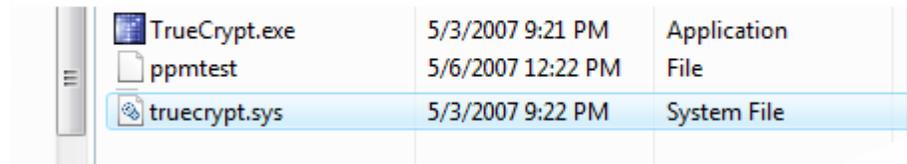
[Statistics](#) (number of downloads)

[Donations](#)

Truecrypt - <http://www.truecrypt.org/>

TrueCrypt

- Lets you use a text file with encryption
- Portable file – again, it fits on a USB, along with the encrypted file.



A screenshot of a Windows file explorer window showing a list of files. The files are: TrueCrypt.exe (Application), ppctest (File), and truecrypt.sys (System File). The file truecrypt.sys is selected and highlighted in blue.

TrueCrypt.exe	5/3/2007 9:21 PM	Application
ppctest	5/6/2007 12:22 PM	File
truecrypt.sys	5/3/2007 9:22 PM	System File

Truecrypt lets you put your “secrets” file on a USB drive, and access it:

The screenshot shows a Windows desktop environment. In the foreground, the TrueCrypt application window is open, displaying a list of drives. Drive F: is selected, showing a volume of 3.0 MB encrypted with Twofish. Below the list are buttons for 'Create Volume', 'Volume Properties...', and 'Wipe Cache'. The 'Volume' section shows 'E:\stuff\ppmtest' selected with the 'Never save history' checkbox checked. At the bottom are buttons for 'Dismount', 'Auto-Mount Devices', 'Dismount All', and 'Exit'.

In the background, a Windows Explorer window shows the contents of Local Disk (F:). It contains two text files: 'crazy.txt' (modified 5/6/2007 12:23 PM) and 'secret-words.txt' (modified 5/8/2007 2:37 PM).

A Notepad window titled 'secret-words.txt - Notepad' is open in the foreground, displaying the following text:

```
File Edit Format View Help
Aliis si licet, tibi non licet.
    Even though it is permitted for others, it
Mundus vult decipi, ergo decipiatur.
    The world wants to be betrayed, therefore
Divide et impera.
    Divide and rule. (Louis XI; adopted by
Nihil sub sole novum!
    Nothing under the sun is new
    Eccl 1:10
Considerate lilia agri!
```

NOTE

If you do use a program like notepad.exe to save an encrypted file using a filesystem like TrueCrypt, there is always the chance that you may leave behind “tracks” in your UN-encrypted filesystem.

This should NOT be used on a shared system, or one where you cannot reliably say you are the *only* user.

Locknote

STEGANOS

Privacy Software made easy.™

COMPANY PRODUCTS PARTNERS CUSTOMER SERVICE TV AD

INTERNATIONAL 

Steganos® LockNote

Steganos LockNote will change the way you work with confidential notes. Application and document in one: the mechanism to encrypt and decrypt a note is part of it. Secure, simple, independent. No installation required.

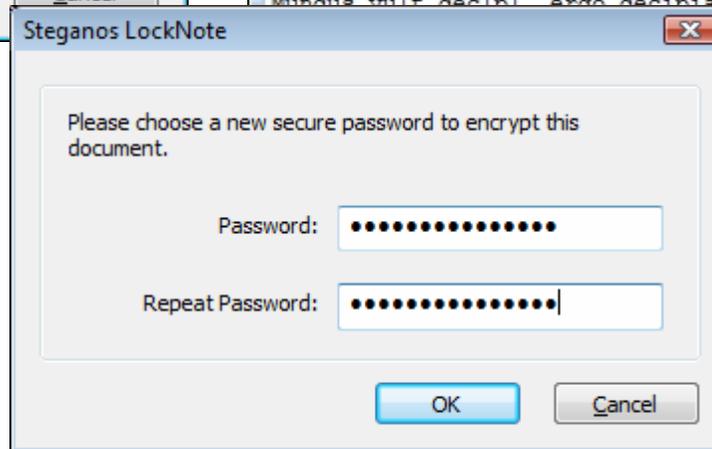
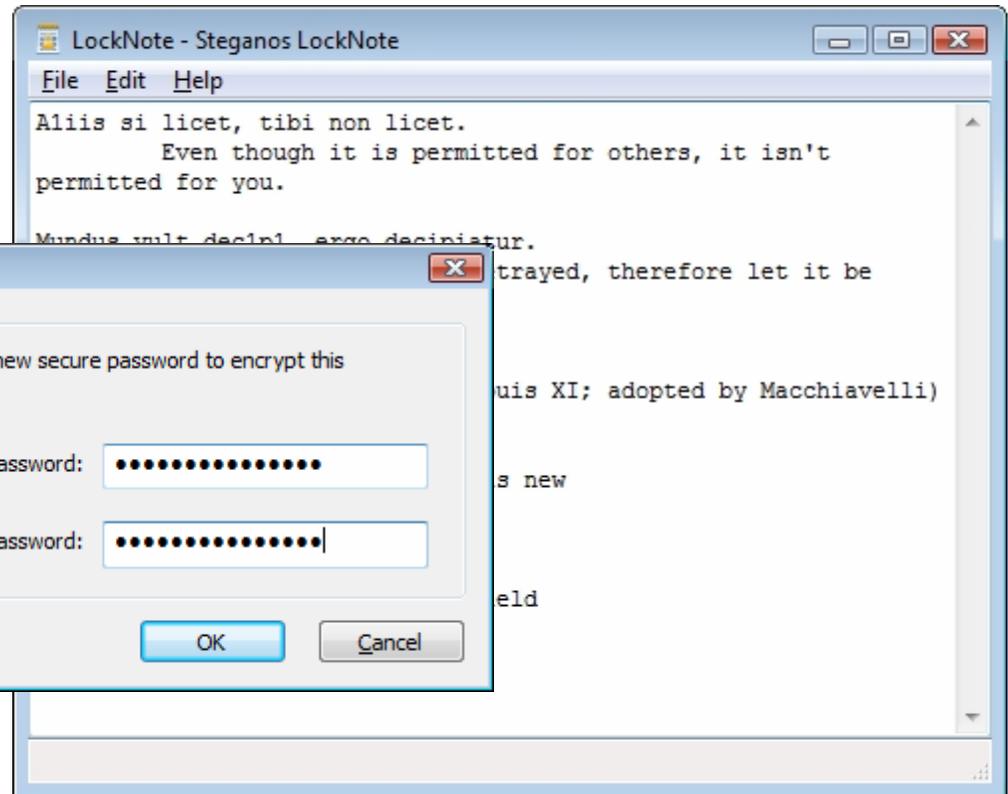
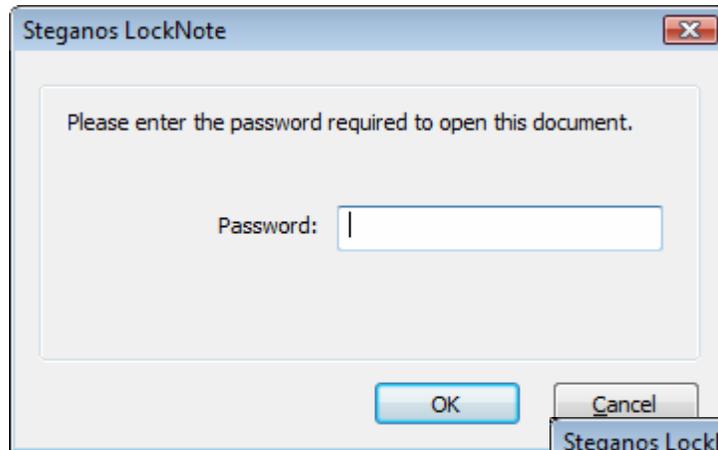
System requirements: Windows 2000, Windows XP or better



Locknote - <http://locknote.steganos.com/>

<http://sourceforge.net/projects/locknote>

As easy (and simple) as NOTEPAD



(just be sure you
remember the
passphrase!)

Choices for the Mac

The screenshot shows the Nirlog.com website. At the top left is the logo "NIRLOG.COM" with the tagline "Technology, Life and other stuff that come along...". To the right is an orange RSS feed icon. Below the header is a blue banner with the text "Welcome to Nirlog.com" and "Actually this is just another wordpress blog... where I write about Technology, Life and anything that I find interesting." with a "Read more" link.

A navigation menu contains links for Home, SecurityTNT, Nirlog Store, About, I Read, Contact, Archives, and Popular. Below the menu is a breadcrumb trail: "Home > Password Managers for OS X".

On the left is a "Pages" sidebar with links to Home, About, I Read, Contact, and Archives. The main content area features a post titled "Password Managers for OS X" by Niranjan Kunwar, dated July 19th, 2006. The post text begins with "I've switched to a Mac and it took quite some time for me to find an ideal password management tool. Of course OS X has an excellent KeyChain Access for password and other confidential information management. Also there are some third party".

On the right is a Google search widget with a search bar, a "GO!" button, and radio buttons for "Web" and "Nirlog.com".

Mac Password Keepers

<http://nirlog.com/2006/07/19/password-managers-for-os-x/>
<http://www.takecontrolbooks.com/passwords-macosx.html>

References:

Password Attack Discussion & Benchmarks by Alan Amesbury,

<http://www1.umn.edu/oit/security/passwordattackdiscussion.html>

Password Memorability and Security: Empirical Results

http://homepages.cs.ncl.ac.uk/jeff.yan/jyan_ieee_pwd.pdf

Strong Passwords: How to create and use them

<http://www.microsoft.com/athome/security/privacy/password.mspix>

Password Strength Tests:

<http://www.securitystats.com/tools/password.php>

http://www.microsoft.com/athome/security/privacy/password_checker.mspix

The Strong Password Dilemma

<http://www.smat.us/sanity/pwdilemma.html>

Tools:

Password Safe - <http://passwordsafe.sourceforge.net/>

Pwsafe - <http://nsd.dyndns.org/pwsafe/>

Password Gorilla - <http://www.fpx.de/fp/Software/Gorilla/>

Truecrypt - <http://www.truecrypt.org/>

Locknote - <http://locknote.steganos.com/>

<http://sourceforge.net/projects/locknote>

Mac Password Keepers - <http://nirlog.com/2006/07/19/password-managers-for-os-x/>

<http://www.takecontrolbooks.com/passwords-macosx.html>