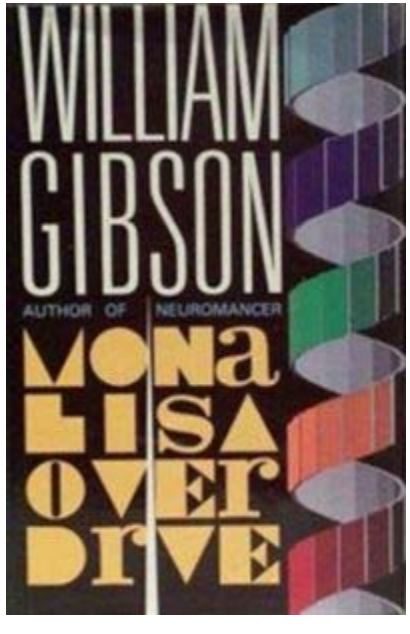
Password Management Ideas

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

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

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".

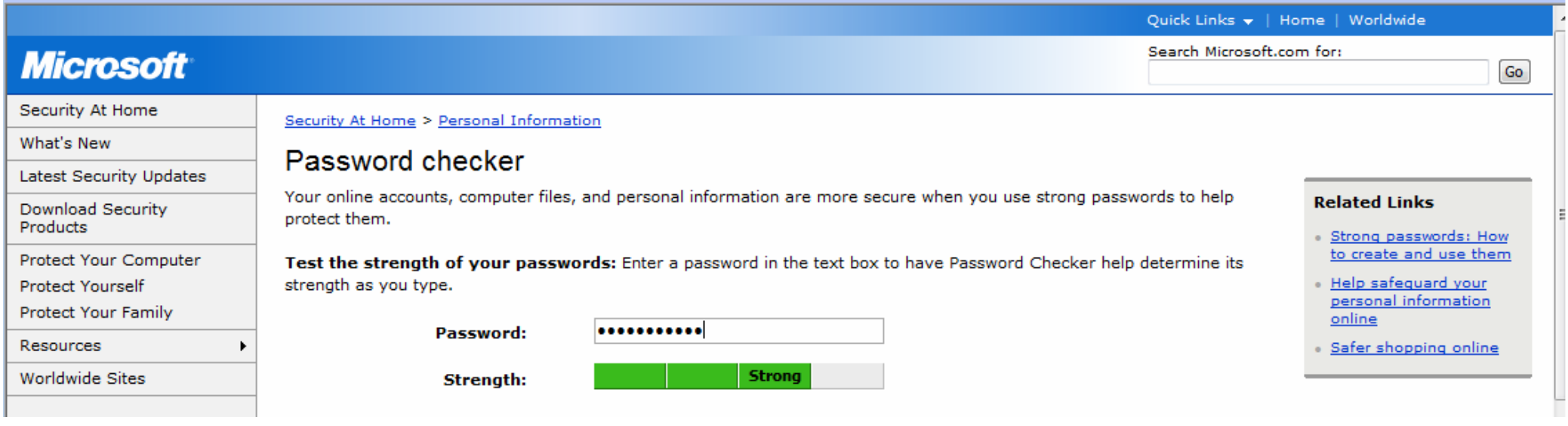
4. Add complexity by mixing uppercase and lowercase letters and numbers. ... This might yield a password like "MsAy3yo".

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.mspx

Offline test (requires ***javascript***) :



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

Online (php based) test:

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!

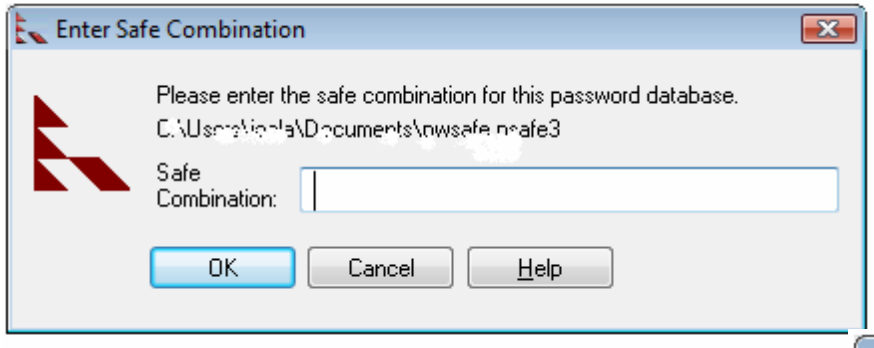
[click here for latest version]

- Latest news
- Non-English versions
- Discussion forum
- Project summary page
- History
- Related projects (other platforms)
- Links

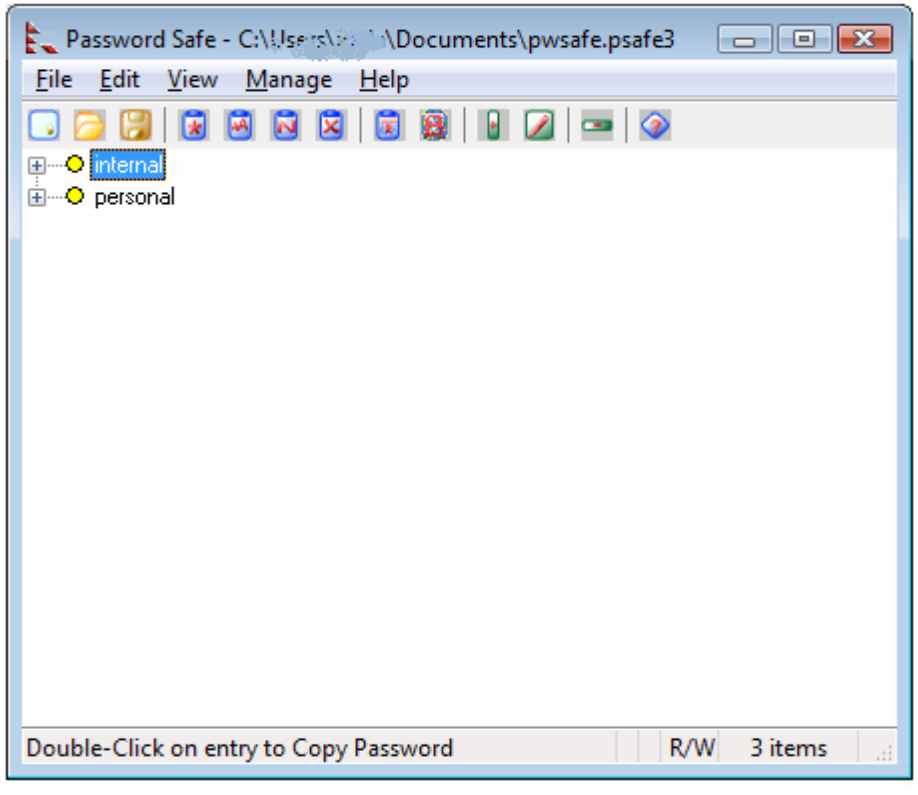
Some testimonials from users:

- *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...

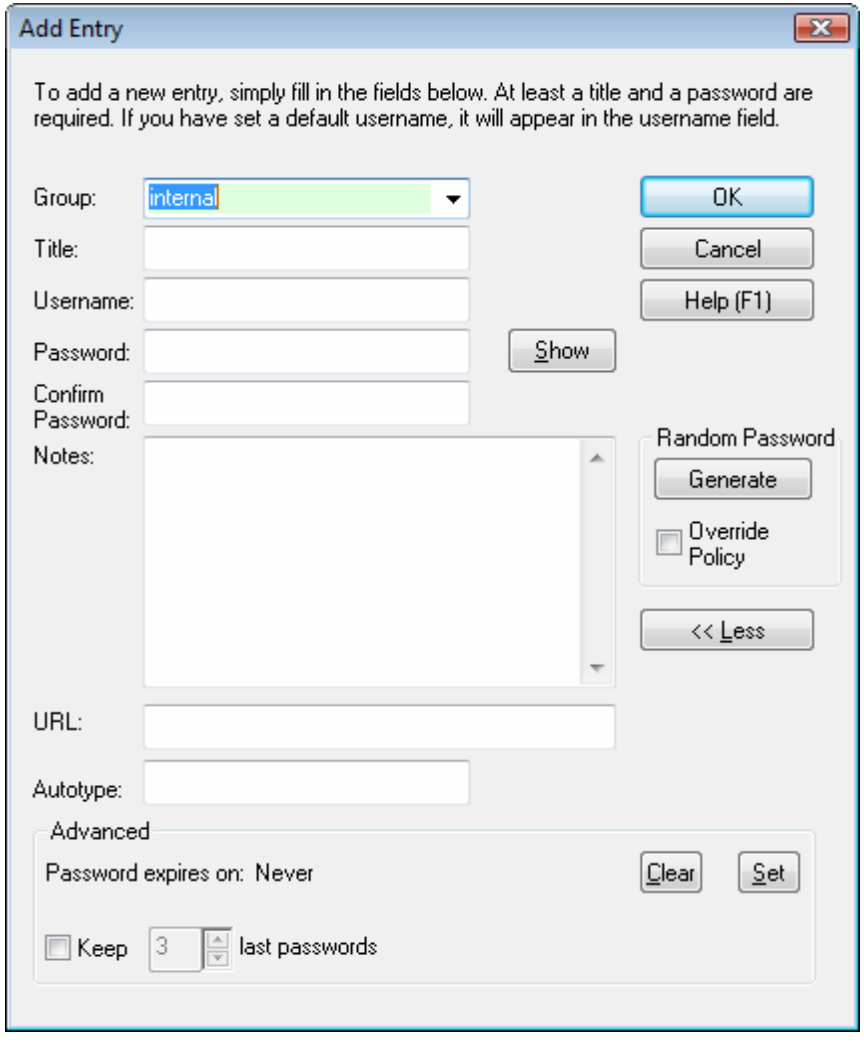
Password access

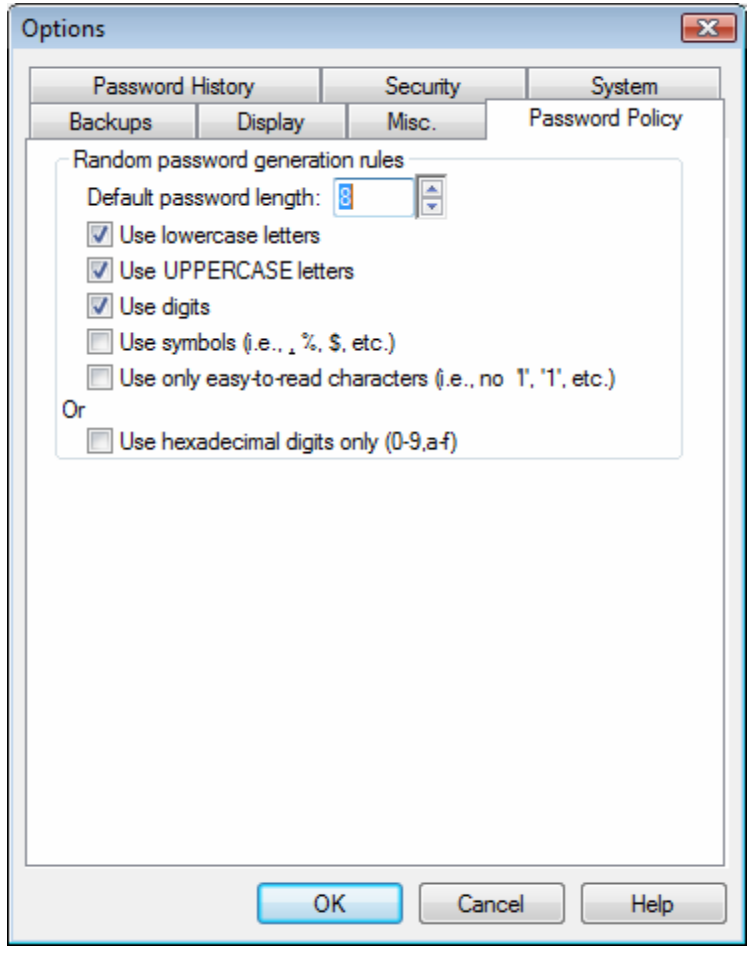


To multiple accounts:

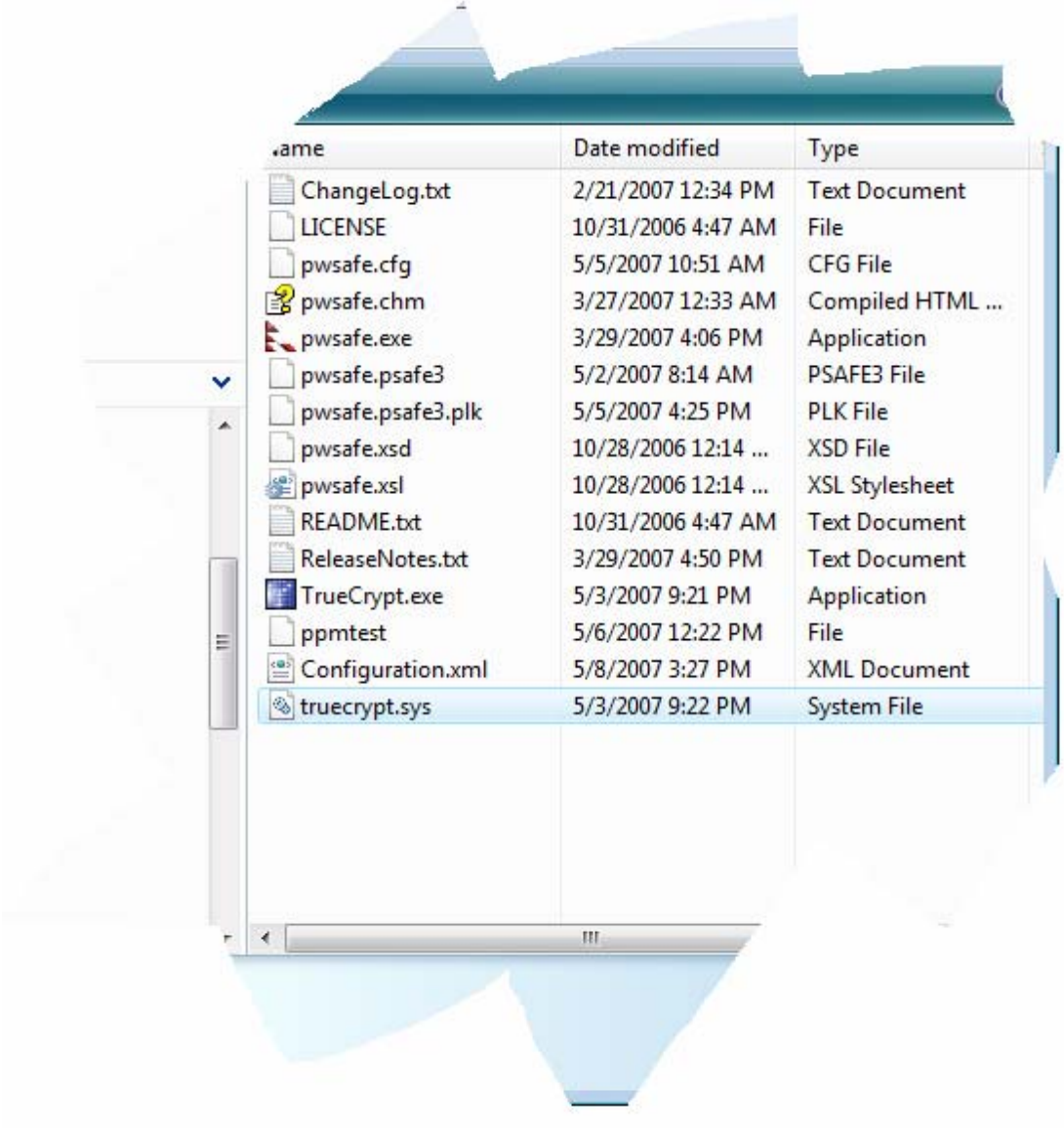


Multiple useful features





Easy to install on a USB drive:



ame	Date modified	Type
ChangeLog.txt	2/21/2007 12:34 PM	Text Document
LICENSE	10/31/2006 4:47 AM	File
pwsafe.cfg	5/5/2007 10:51 AM	CFG File
pwsafe.chm	3/27/2007 12:33 AM	Compiled HTML ...
pwsafe.exe	3/29/2007 4:06 PM	Application
pwsafe.psafe3	5/2/2007 8:14 AM	PSAFE3 File
pwsafe.psafe3.plk	5/5/2007 4:25 PM	PLK File
pwsafe.xsd	10/28/2006 12:14 ...	XSD File
pwsafe.xsl	10/28/2006 12:14 ...	XSL Stylesheet
README.txt	10/31/2006 4:47 AM	Text Document
ReleaseNotes.txt	3/29/2007 4:50 PM	Text Document
TrueCrypt.exe	5/3/2007 9:21 PM	Application
ppmtest	5/6/2007 12:22 PM	File
Configuration.xml	5/8/2007 3:27 PM	XML Document
truecrypt.sys	5/3/2007 9:22 PM	System File

Other Developments

Pwsafe – command line version for multiple OS's

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

Password Gorilla

A cross-platform Password Manager

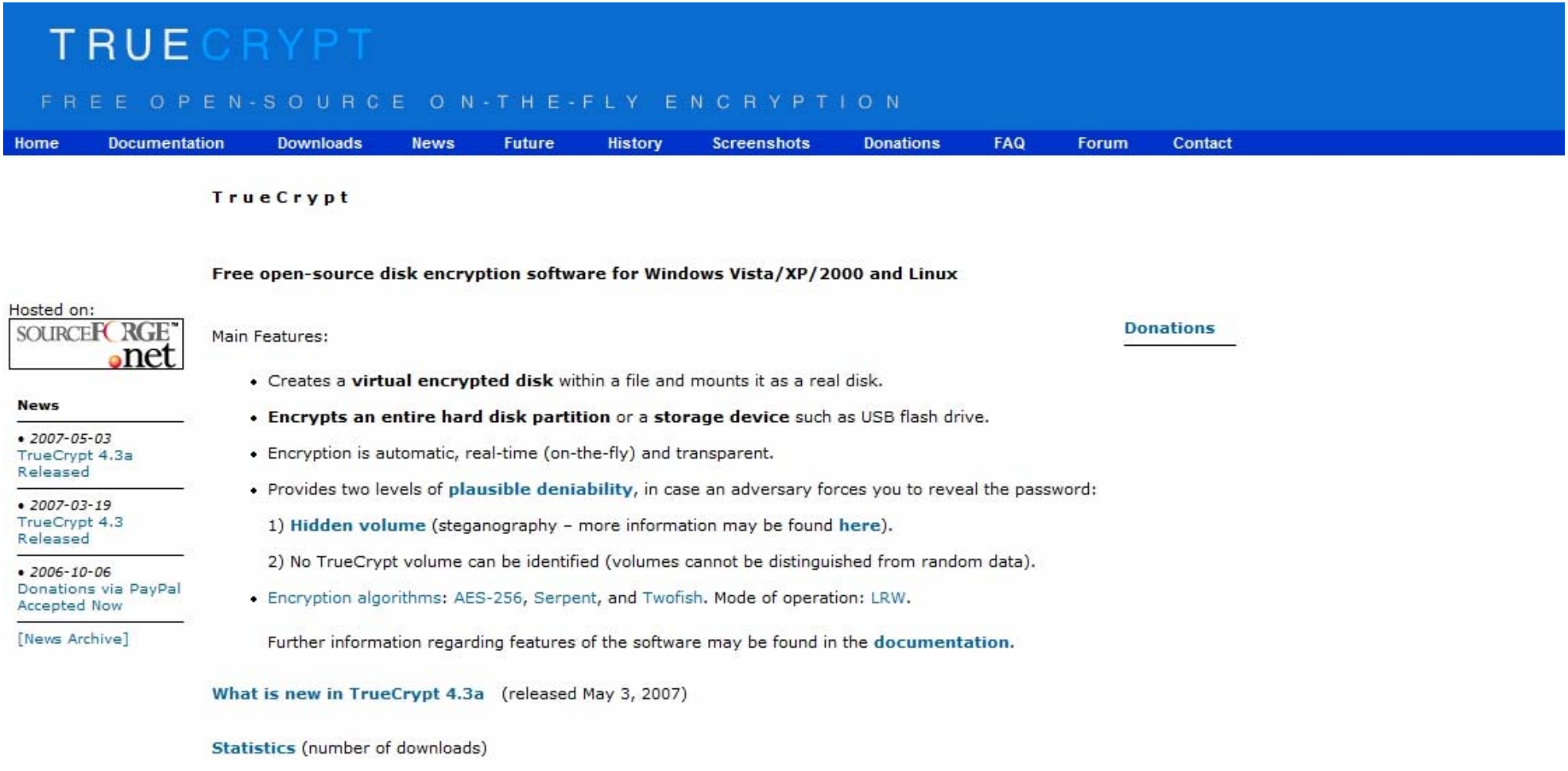
Now Available for Microsoft Windows, Mac OS X, Linux, Solaris, *BSD, etc.

Free, Open Source Software!

Version 1.4

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

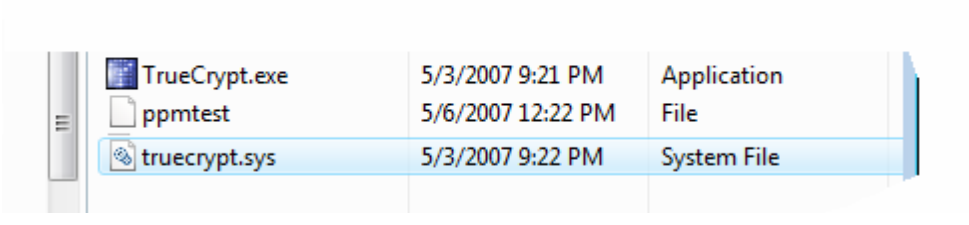
TrueCrypt



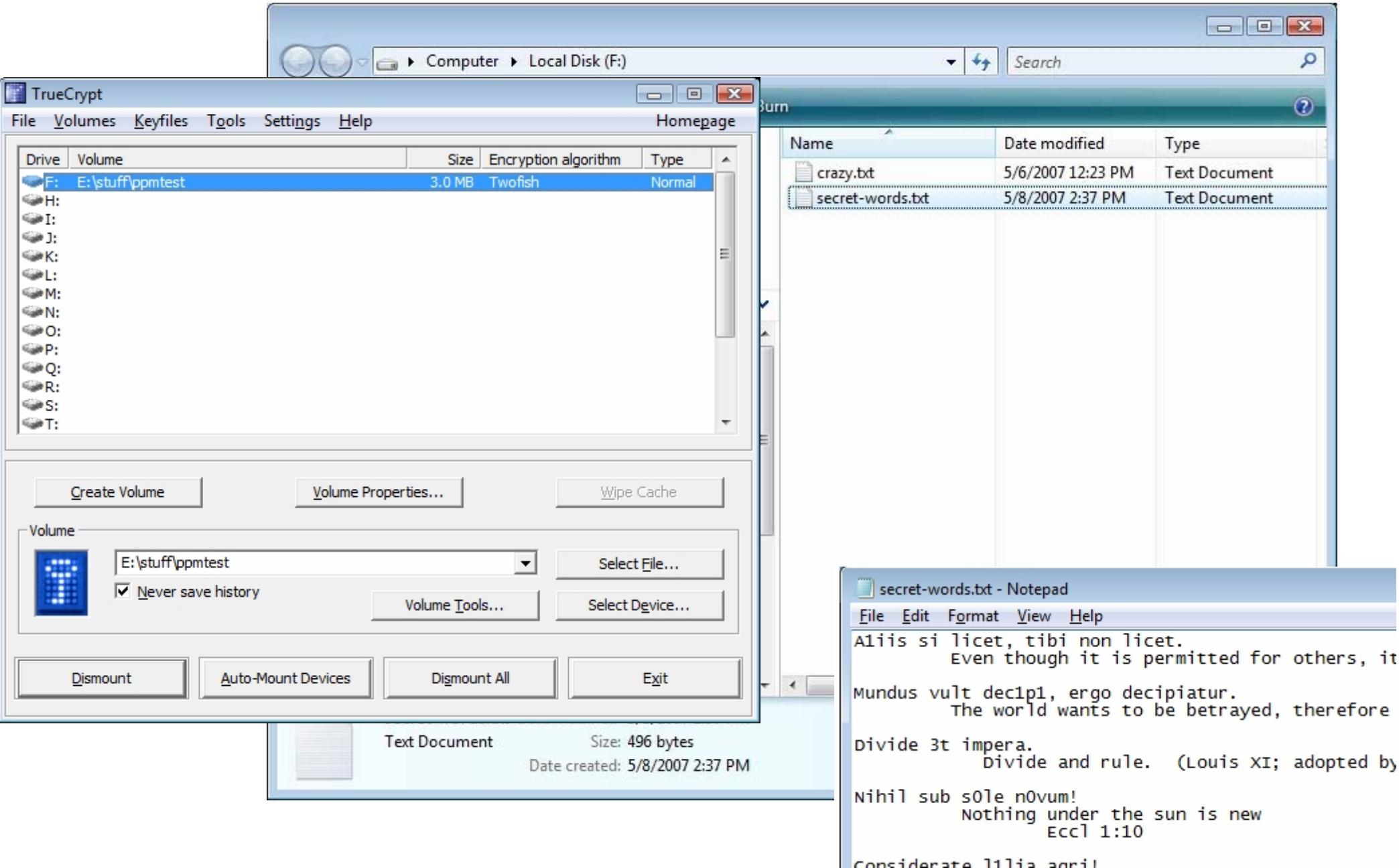
Truecrypt - http://www.truecrypt.org/

TrueCrypt

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



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

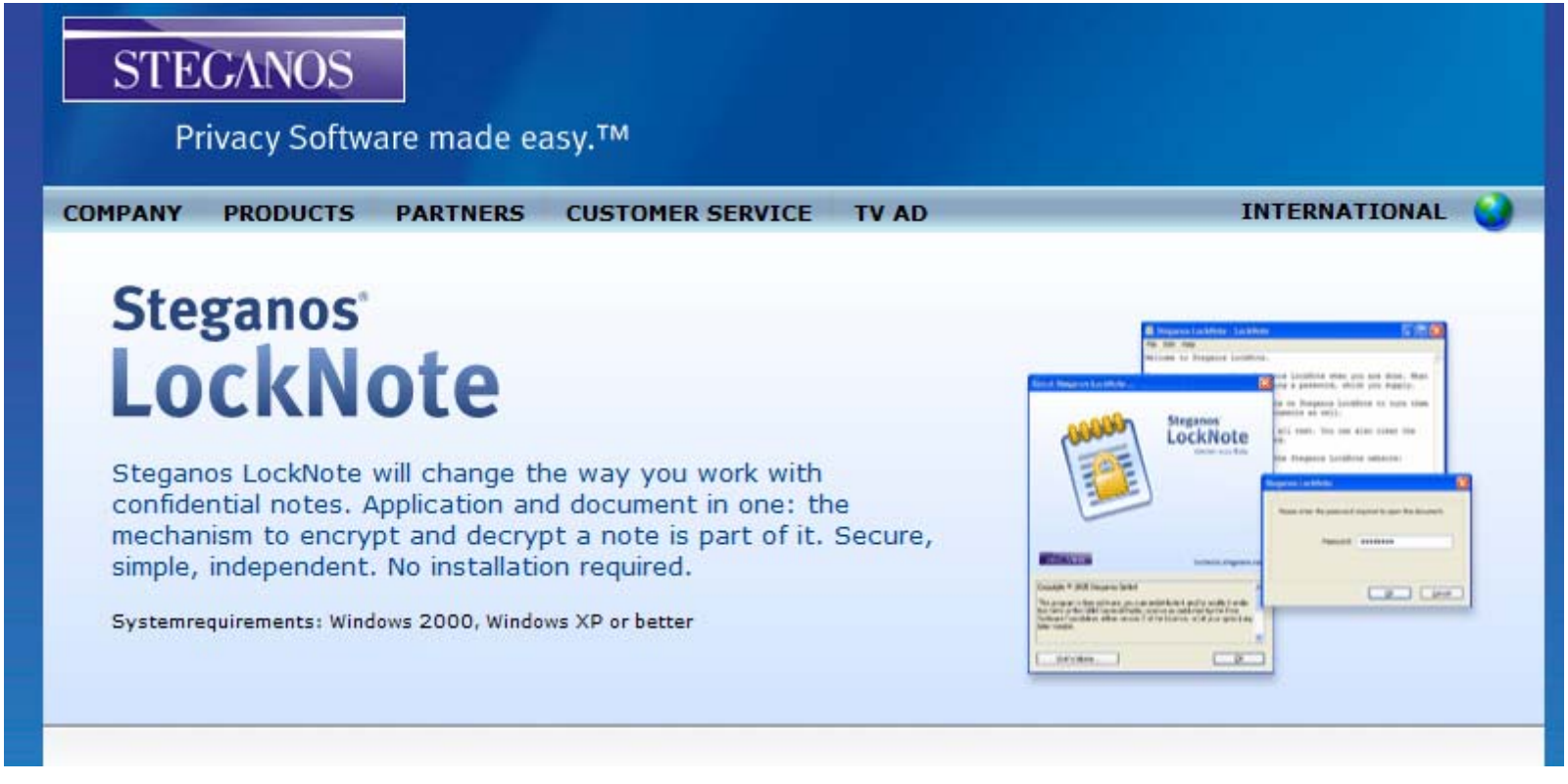


NOTE

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.

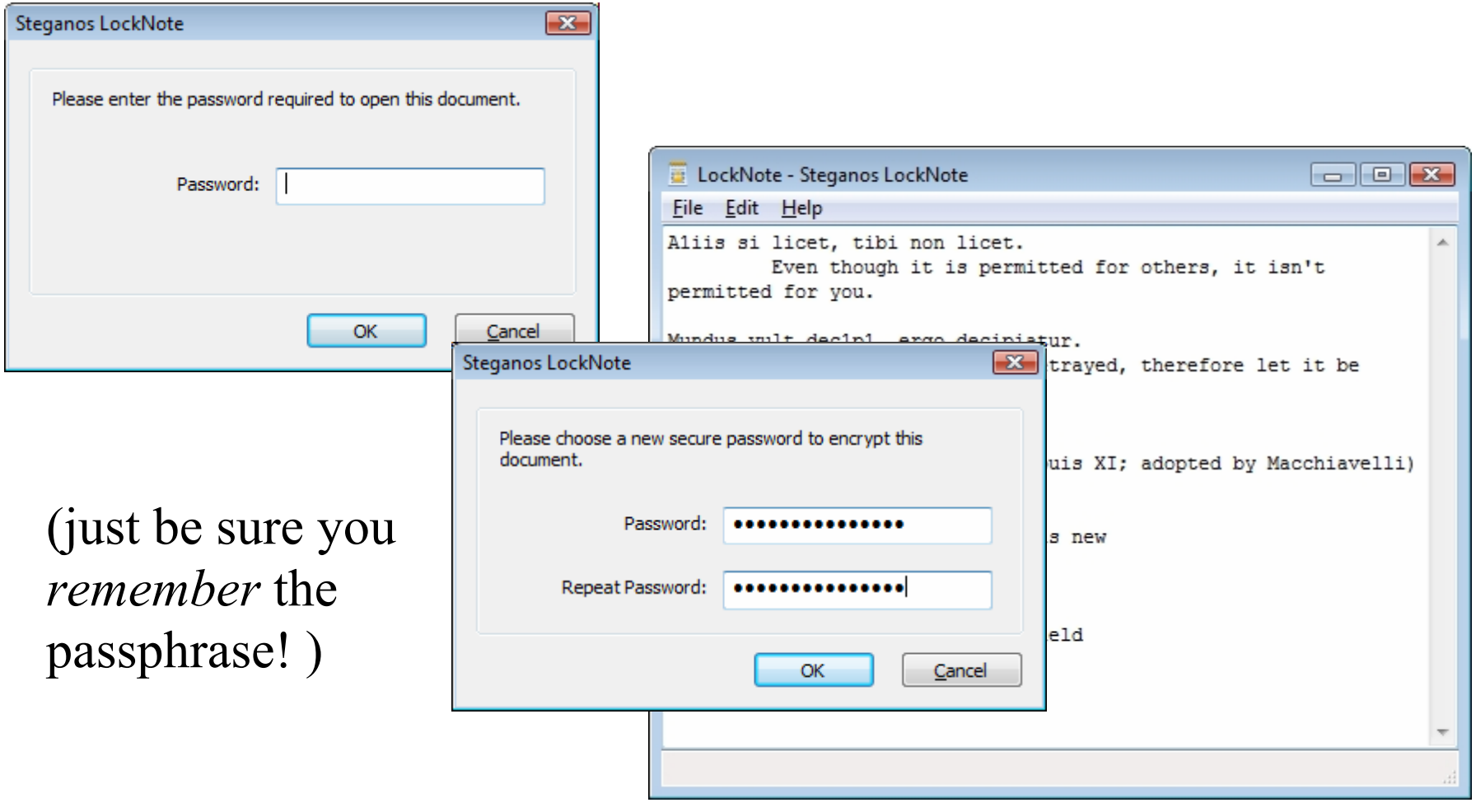
Locknote



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

http://sourceforge.net/projects/locknote

As easy (and simple) as NOTEPAD



(just be sure you *remember* the passphrase!)

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

Choices for the Mac

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.mspx

Password Strength Tests:
http://www.securitystats.com/tools/password.php
http://www.microsoft.com/athome/security/privacy/password_checker.mspx

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