

KeySafe v0.1 *Alpha II*

Introduction

KeySafe is an application used for the safe storage of passwords of a local hard disk.

To achieve a greater level of security, date encryption and hashing functions have been added to the program. The algorithms present in these functions are not 'home grown', but rather, are well known and tested algorithms, which have been heavily scrutinized for security holes over many years. More information on these algorithms are given later in the file.

In modern computers, many username and passwords are needed while on-line on such services as the Internet. Unfortunately, while on-line, and even when off-line, even if you are the only person with physical access to your computers, it may still be exposed to Trojans or key-loggers that may discover your password. KeySafe attempts to counter such programs by flooding these programs with random characters, making it very difficult to find the 'good' characters from the 'bad', and by keeping the password in memory as little as possible.

KeySafe v0.1 Alpha has not yet been fully tested, and we recommend that you do not store any sensitive information within it until further testing can be done.

A Note to Alpha Testers

As an Alpha tester, we ask that you test the following:

- *Add/Remove Key Functions* –
Attempt to confuse the program as much as possible – Use weird names, with ascii characters within them. Try to put as much stress on the program as possible.
- *The 'copy' function* –
Ensure that it works for all passwords, including passwords with non-standard ascii characters within them
- *The startup password screen* –
Install key loggers and/or Trojans onto your computer, and see if they can easily find the password. Report any that can, preferable with the URL to download them. *This feature may be disabled in your revision of KeySafe for computability reasons.*
- *The password scorer* –
Do you think that it is giving fair scores for secure/insecure passwords? Can you find an example of a secure password with a low score, or vice-versa?

Also, while testing, please note that the following features are missing or incomplete:

- Import/Export KeyRing
- Documentation
- Readability password scoring test
- Advanced password scoring systems
- Drag and Drop File Encryption

AlphaII Finish

The AlphaII version of KeySafe v0.1 will expire on 30 March 2000. With luck, you should receive a message from the program informing you of this. If you wish to continue to help testing, or have received the program after this date, please e-mail ravingcow@mail.com for the latest version.

AlphaIII Project Start

AlphaIII Project testing will start on 1 April 2000. It is likely that it will only run for two months, when KeySafe v0.5 Beta will be released to the general public for the first time. AlphaIII will include almost all features complete, lacking only advanced File Encryption Management, and some on-line features of KeySafe.

KeySafe v0.5 Beta

More information will be given later, but it is likely that it will be released some time mid 2000.

Algorithms Used

Algorithms used in KeySafe are:

Hashing Algorithms

Message Digest #2 Hashing Algorithm (MD2)

128 Bit Hash (3.4 x 10³⁸ Possible Combinations)

Algorithm is correct to the RFC1319 Standard when input is less than 16 characters, but a small bug in the code causes the incorrect result when the input length is 16 characters or greater.

Encryption Algorithms

All encryption algorithms are closely based on RC4 and CiperSaber, with slight variations in the 'salt' routines.

Future Algorithms

Algorithms that are likely to be implanted in KeySafe in the future are:

Hashing Algorithms

Message Digest #5 Hashing Algorithms (MD5)

This algorithm is much faster and more secure than the soon-becoming-outdated MD2 hashing algorithm, and after the release of KeySafe v0.5, this will be one of the first features to go in.

Encryption Algorithms

Triple-DES / CAST-256

One of these two encryption algorithms is likely to appear in later versions of KeySafe, but is not a top priority, as RC4 is still considered secure by almost all organisations.

Source Code

The source code to KeySafe v0.1 AlphaII will not be available to the public, but the source code of KeySafe v0.5 Beta will be available to the public for free, although the distribution may be limited. More details will be given closer to the time.

Use of included DLLs and OCXs

The DLLs and OCXs come under the same license of KeySafe, and may be used in non-commercial applications as long as all copyright notices are kept, and David Greenaway and RavingSoft appear in the credits and readme files (if applicable.)

Not guarantees are given that future versions of these files will be backward compatible. For support in using these, please e-mail RavingCow at ravingcow@mail.com.

Copyright

KeySafe is © 2000 by David Greenaway (a.k.a. RavingCow) but may be freely distributed, as long as the program and all included documentation is included unchanged. KeySafe AlphaII or previous versions *should not be used* after 1 January 2001.