PRODUCT REVIEWS

May 20, 1996 (Vol. 18, Issue 21)

Windows password management and encryption

Password Master's security only as strong as its hints
By Joe Peschel

Have you got more passwords and PINs than you can remember? Then consider Password Master, an intriguing password management program from International Systems Inc. This program is useful but not flawless, yet the flaws can be put to good use. Password Master is available in two versions: Version 2.0.5e, which can be exported, and Password Master Pro, Version 3.0.1, which cannot.

If you're already using ViaCrypt's freeware or commercial Pretty Good Privacy, RSA Secure, or any file encryptor whose algorithm is strong to encrypt a file in which you keep track of your passwords, you don't need Password Master.

If, however, you're using something as insecure as a password-protected Microsoft Word or WordPerfect document, a Lotus 1-2-3 or Microsoft Excel spreadsheet, or a PKWare Inc. Zipped and encrypted file to store confidential information about your accounts, read on.

Password Master runs in two modes: master mode for full access and view mode for limited access. Both require passwords. You can specify as many as three hints to remind you of each password.

In master mode you store your account information in a spreadsheet that can hold information about 50 accounts. You enter a description of your account, a log-in name or account data, and hints about your accounts' passwords. (The hints are interesting, but I'll talk about them later.)

Password Master then encrypts your information using DES so that unauthorized persons cannot view your information. Although the company admits that DES, which had a colorful history involving Big Blue, the National Security Agency, and the possibility of DES-cracking machines, can likely be cracked by major governments, it's a fairly strong encryption algorithm. It is implemented using Bokler Software Corp.'s DESCypher VBX tools. (Bokler, on its Web site, http://www.hiwaay.net/bokler, demonstrates the triviality of some encryption schemes by linking to password-cracking programs for Word and other programs.)

After data is encrypted, the master mode lets you display or hide data. You can use the view mode to select your application and get hints

about application passwords.

The hints, although an intriguing idea, are a major source of concern. They can be used for the program's own master and view modes and for all of the applications.

If I give myself good hints to help me remember, for instance, the master password, what's to prevent someone else from looking over my shoulder and solving the password puzzle? Even if the hint is personal, it might be swiped by Mitnickian "social engineering." This is a problem with every hinted password.

What's worse is that hints appear as plain text in otherwise encrypted data files. How do you give hints about strong pass-phrases such as rudf4\vLdor$tUDr, anyway? My solution: Do not use any hints for the master password -- remember it; and use spurious hints for the application data to mislead attackers.

The not-for-export version, which the company rushed to me after hearing some of my concerns, allows 200 fields for data and encrypts the application hints but not the hints about the master and view passwords. You can also disable hints in view mode.

The freeware alternative

An alternative to Password Master is PassKeeper, freeware written by Brad Greenlee, with an implementation of triple DES by Eric Young. Triple DES is harder to break using an exhaustive key search: 2112 attempts compared with 256 attempts.

PassKeeper lacks the bells, hints, whistles, and cute little icons of Password Master, but it lets you store data for 128 accounts, compared with Password Master's 50, and it includes a field for notes. Plus, it can be installed in several directories, allowing you to store information on as many accounts as you have the disk space to track. Both 32- and 16-bit versions can be found at: http://www.isys.hu/staff/brad/passkeeper.html.

Joe Peschel covers single-system security products and other stand-alone utilities. He can be reached at jpeschel@aol.com.

THE BOTTOM LINE: GOOD

Password Master, Version 2.0.5e (exportable) and Password Master Pro,Version 3.0.1 (not for export)

Password Master is an interesting utility for storing passwords whose uniqueness is its weakness.

Pros: Easy-to-use spreadsheets for entering application data; hinting mechanism that can be used for thwarting attackers but isn't intended for that.

Cons: Hints that are otherwise a security flaw, some in plain text.

International Systems Inc., Chicago; (800) 248-4217, (312) 222-1364; fax: (312) 222-9226; us016835@interramp.com; http://www.isi.inter.net.

Price: $29.95

Platforms: Windows 3.x, Windows 95.

Copyright (c) InfoWorld Publishing Company 1996