Contents

Welcome to Password Spy

Password Spy is a freeware utility that looks inside WinCIM or CisNav to find any passwords that you have, decrypts them back to their original state and tells you what they are. WinCIM and CisNav encrypt these password(s) on your hard disk to avoid casual snooping.

This utility is designed to be used when you've forgotten what your password is, but you want to change it. Previously if you forgot your password, you couldn't change it without getting CompuServe to issue you with a new password, a lengthy and inconvenient procedure. Now you can recover your original password(s).

Please do not misuse this utility. It is NOT clever to appropriate other peoples' accounts.

Procedures

Reference

Using Password Spy

When Password Spy first starts, it looks for a WinCim/CisNav file called CIS.INI, usually in the C:\CSERVE directory. If it can't find it, it prompts you to specify where it can be found. Once located, Password Spy always remembers where it can be found.

Once it has located CIS.INI, password decryption is automatic. The first account displayed is always the Current Active Session in WinCIM or CisNav. Other accounts and passwords are displayed after a blank line.

That's all there is to it! You can print the account and password details if you wish.

The other additional tip is that you can specify the path to CIS.INI as a command-line property (in Program Manager) if you wish.

Menus

File Menu

PRINT PASSWORDS
This prints any passwords found to your default printer. If there is a printer error, you get a chance to retry printing or to just ignore the error.

COPY PASSWORDS
This copies any passwords found to the Windows Clipboard.

EXIT
This ends Password Spy, of course, by way of a goodbye dialog.

Help Menu

CONTENTS
This displays the first (contents) page of the Help file.

SEARCH
This displays a Search dialog enabling you to look for keywords in the Help file.

ABOUT
This displays an About dialog showing product copyright details and information about your registered name and company.

Keyboard

Keyboard Shortcuts

ESCAPE
Ends Password Spy.

CTL-P
Prints any password(s) found to the default printer.

CTL-C
Copies any password(s) found to the Windows Clipboard.

ALT-P
Prints any password(s) found to the default printer.

ALT-E
Displays the Help file (contents page).

ALT-A
Displays the About dialog

ALT-X
Ends Password Spy.

ALT-F
Displays the File menu.

ALT-H
Displays the Help menu.

How Does The Decryption Work?

The first thing to notice is that WinCIM (and CisNav) stores your password(s) in CIS.INI, encrypted into a hexadecimal format.

I used a plaintext attack, writing a Visual Basic program to type in a large range of passwords and then storing the encrypted passwords that WinCIM produced. I then wrote another program that compared what went in with what came out, and produced a table of the results. Manual analysis of, and experimentation with, this table showed how the encryption algorithm works.

What happens is that each character of your password is XORed with a arbitrary character that WinCIM has stored, and then converted to hex. WinCIM has 17 of these characters, and cracking the password is simply a case of working out what they are.
As a password can be a maximum of 24 characters long, after 17 characters of the password have been processed WimCIM starts with the first character again. CHR$(0) signifies the end of the password, if it's less than 24 characters long.

So for each encrypted hex character :-

DecryptedCharacter = EncryptedCharacter XOR ArbitraryCharacter(1-17, repeating)

What are the 17 arbitrary characters that are used? That would be telling <grin>.

About The Author

My name is Mark Pearce. I'm the managing director of a 3-person company (Sleek Software) specialising in banking and security software. I've also written a freeware program which decrypts Word for Windows (version 2 & 6) documents when the password has been lost, and I'm working on PKZip decryption.

I wrote Password Spy simply because I forgot my WinCIM password. It took me a couple of days to figure out how the passwords are encrypted, and I wrote this program to implement the decryption during an 18 hours' stint at the keyboard, using Visual Basic 3 Pro.

Password Spy is freeware, but I would appreciate an e-mail if you find it useful.My CompuServe address is 100272,2353. If you're paranoid, or indeed if they're really out to get you, my PGP key is at the end of this Help file.

PGP key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAi2wuN4AAAEEAM2YpenyoqululQ1Oci+rmJIQP6QnYgMF3T34ARLhhCzfXuw
pShbT+GRKyucGJAA9On3KywsKRk/Bg3ZCdvp49ohCItcp1rTaV8FzaCdhu9Htolb
fvCWikaCRk5GB/qOUMGdD12JX4KpVyrJ9r0RIw1bNuxLnTUMsZ0ddPqqIN91AAUR
tCpNYXJrIFMgUGVhcmNlIDwxMDAyNzIsMjM1M0Bjb21wdXNlcnZlLmNvbT6JAJUC
BRAtuhannR10+qog33UBAXoZA/9/vrveEtsbcrCp3pd/AFuZglL5JI8VePen6960
X8kNSpbbg8y4DX6PBTlO65GksuRnlClSwg5l4IbO5/QypkHwn0AWFFaGEq4oTn4M
+qV29SIgy+7JoEjBvoUu4qhGpIiWjRs5gIwYCXYmhM8r1Vvdphs0lzLu2+xWa06Y
hgsLlQ==
=phMH
-----END PGP PUBLIC KEY BLOCK-----

How Does the Decryption Work

<How Does The Decryption Work>

PGP key
<PGP key>