etting Passwords with Macsbug
By Astrosmurf

Intro

Have you ever seen a program that has a password entry field, but it looks like "••••••••"? It is VERY unlikely that you haven't. One example is in Remote Access (Fig. 1.) The login name and dialup number are clearly visible, but the password is blanked out. How annoying. There are, however, ways of getting past this. In this paper I shall describe the two main methods that I can think of.

ig. 1 - The remote access control panel. Pay particular attention to the buletted password field.

The Hard Way

If the program shows the password even after you have restarted the program, then the password is stored in the application's preferences. So you just need to open up the preferences file for that program in resedit, right? Well, that's the easy part. You then need to find where the password is stored in the preferences.

In many cases you just need to look for a resource called "pass" or "pwrd" or something. However, it might not be so obvious where it is. Naming the resource "pass" isn't very secure as anyone opening up the prefs file will see it and open it up, bringing them one step, or possibly all the way towards finding the password. The person making the application may. however, realise this and decide to confuse you by calling it something unrelated, or mixing it in with other data. If they really want to confuse you, they'll make a fake resource called "pass" and put some false data in it, sending you on a wild goose chase.

If you find where the password is hidden, it's probably encrypted. It would be silly otherwise. Sometimes this encryption is easy to crack, but it can just as easily be annoyingly difficult. The encryption method will almost certainly be two-way: If the program needs the use the password itself (for example Remote Access) then it has to be two-way, because the program has to be able to decrypt the password without any input from the user. The simplest encryption for a stored password that I can think of was in At Ease 2. A few years ago, I wanted to know how to get the passwords from the prefs files, so i set the password for a user to "abcdefgh" or something and went into resedit to look for this. I then changed the password again, went back to resedit and looked for anything that had changed. I then realised that the password was encrypted with a simple substitution. I had soon made up a list of the substitution values, and had found another flaw in At Ease.

If, however, the encryption is stronger than this, you could spend hours upon hours trying to get the password, but not get any closer. Thankfully, there is a much easier way.

The Easy Way

Yes, there is a much easier way of getting blanked out passwords. But how? Well, while the program is running, the password must be in your computer's memory somewhere. You could drop into MacsBug and search for the password, but you'd need to know the password to do this (which makes it a bit pointless). If we search, we need to know what to search for. So, you simply need to edit the password. Click at the start of the password and enter in an uncommon string of letters (using something like "mem" is a bit silly). Then drop into macsbug and search for it:

F 0 FFFFFFFF 'whateveryoutyped'

After a while, it should tell you that it's found the string and, if you look, the password should be hanging off the end of it. Well, done! You now have the password.

Why It Might Not Work

This will almost certainly work with things such as Remote Access, ICQ...
It is a bit harder if the length of the password is limited (such as in ICQ) as you may not be able to enter any text yourself. What you need to do is make a copy of the prefs (or the user setup for ICQ) and run the program. You then delete a few letters from the end of the password and type your own at the beginning. Search for this and you will find the first few letters of the password. Replace the original prefs and search for these new letters, and you will have the whole password.

If the program needs you to enter the original password in order to alter it, you might be stuck.

Astrosmurf
astrosmurf@iname.com