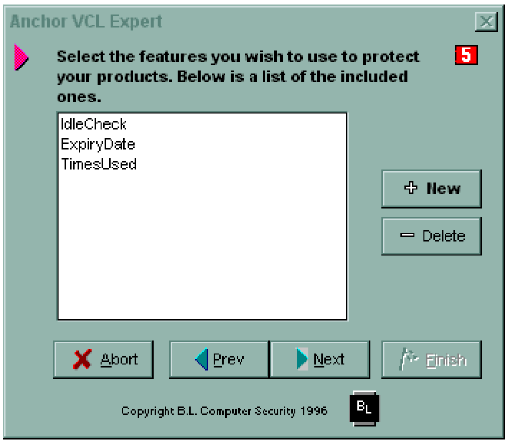
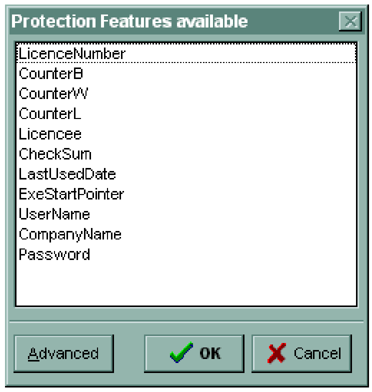
Review: Anchor-P Copy Protection

by Dave Jewell





Copy protection is an issue which most software developers have to worry about from time to time. Whether you need to copy protect a particular application depends on the type of software, its market and price. Copy protection is most often used to protect high-cost, low-volume, vertical market software such as electronic CAD.

Anchor-P, from BL Computer Security, is an interesting copy protection product aimed specifically at Delphi developers. It uses a small hardware 'dongle' (BL prefer the term 'key') which fits into a PC's parallel port. The dongle has standard 25-pin male and female D-type connectors at each end so that you can still plug your printer in. It contains a dedicated processor chip which can allegedly retain data for up to 100 years without being plugged in to a PC. It includes 512 bytes of read/write memory and three levels of password protection. Normally, the dongle is transparent to the operation of the parallel port and ignores any data sent to the printer. However, if it recognises one of its own instructions together with a valid password it responds accordingly. Since a particular dongle will only respond to its own passwords, you can daisy-chain multiple dongles on the same port if needed.

All this is pretty standard stuff, so what makes Anchor-P of particular interest to Delphi users? Does it come with a snazzy VCL component to access the dongle's capabilities? Funnily enough, no. What you actually get is the Anchor VCL Expert which can be installed into Delphi in the usual way. Using this expert, you get asked a series of questions about what protection capabilities you need and it then generates a source code file which can be compiled into a new non-visual component ready for inclusion in your own applications.

There a number of distinct advantages to this approach, one of them being that 'rolling your own' allows you to create components optimised to each project.

In terms of functionality, the designers of the component seem to have covered most of the bases. For example, you can use `IdleCheck` which hooks into the `TApplication.OnIdle` event, periodically checking that the dongle is still installed. This is important, because a popular technique for defeating dongles is to launch the software on one machine with the dongle plugged in, then put the dongle into another PC and repeat the process. With `IdleCheck`, this will be noticed very quickly, so you can then take whatever action you think best...

Even more powerful than this is the ability to read and write your own data to the dongle's memory. You might use this to implement a usage count so that demo software will only operate a certain number of times. Without a dongle, most software authors place the counter into the Windows registry, on the hard disk, or even in the EXE file. All these techniques can be defeated by reinstalling another copy of the software onto another PC. With the dongle, that's a no-no.

Of course, most copy protection schemes can ultimately be defeated by tracking down all the branch instructions where the software decides whether or not a dongle is installed. For this reason, if you want ultimate protection, you might consider storing small chunks of program code on the dongle and only loading them into memory transiently at critical points in your program's execution. This needs careful thought because the dongle is quite slow at responding to commands, (around 15ms) and you don't want to introduce a performance bottleneck.

The versatility of this package is such that you can implement simple security schemes and very complex ones: you should really think of Anchor-P as a copy protection tool-kit. You do need to be mindful of the 15ms delay needed to interrogate the dongle though. Currently, Anchor-P is only available for 16-bit Delphi, but a 32-bit version is in the works. Once this becomes available, it would make sense to use another thread to take care of 'dongle sniffing' and leave the user interface thread to run at full speed.

A Developer Pack including two blank keys and documentation costs £69. Further keys can be obtained priced at £25 each in quantities of 10, down to £17 each for 1,000. For details, call BL Computer Security on +44 (0)181 343 0734, email info@blcs.co.uk or visit http://www.blcs.co.uk.

Dave Jewell is a freelance consultant and technical journalist (email DaveJewell@msn.com)