

Re: FileCopy overwrites the existing file

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-12/msg00297.htm>

- *From:* Grzegorz Wróbel </dev/[null@xxxxxxxxxxxxxxxxxxxxxx](mailto:xxxxxx@xxxxxxxxxxxxxxxxxxxxxx)>
 - *Date:* Sun, 10 Dec 2006 20:14:09 +0100
-

anton bassov wrote:

Pavel,

But what about the performance penalties that you are guaranteed to encounter if you implement encryption at so low level???

My Thinkpad laptop has disk encryption, probably it is done in the ide controller. The disk performs not worse than in other models.

I think it mainly depends on the encryption scheme.....

Have you got any idea about the encryption scheme that your laptop uses? I think that, because of government regulations, it must be something not-so-strong, so that your disk can be decrypted by someone with a special equipment pretty easily.....

However, imagine if you used 1024-bit or 2048-bit encryption – how fast would it be???

For symmetric encryption 256bit is far beyond the reach of anyone to decrypt, with good algorithm even 128bit is considered secure. And these algorithms (symmetric) are fast as hell, here even large key wouldn't be a problem. 1024 or 2048bit key encryption is needed for non-symmetric encryption schemes like RSA. And this algorithm is slow, because it requires specific numerical operations (ie raising to the power modulo) using 1024-bit or 2048bit integer numbers.

—
Grzegorz Wróbel
<http://www.4neurons.com/>

Re: FileCopy overwrites the existing file

677265676F727940346E6575726F6E732E636F6D

.