

## NovaStor's Decision to Utilize the Blowfish Algorithm

Blowfish, designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms, is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

A number of key factors contributed to NovaStor's decision to incorporate the Blowfish encryption algorithm into our NovaNet-WEB product:

- Blowfish is classified as public domain; as such it has been analyzed extensively and gone through years of peer review. At no point since its initial release in 1993 has the Blowfish code been cracked. This is significant when you consider that the source code to the algorithm is freely available. This supports one of the most important aspects of any good encryption algorithm.
- Blowfish supports key lengths of 38 to 448 bits making it one of the strongest encryption algorithms on the market. (Since the US government (NSA) has eliminated export restrictions on encryption, NovaStor now ships NovaNet-WEB with 448-bit support standard.

The relative strength of the encryption algorithm is based on key length. Bruce Schneier, creator of the Blowfish encryption algorithm, has calculated that according to what we know of quantum mechanics today, that the entire energy output of the sun is insufficient to break a 197-bit key.

Here is a more generalized example:

The most common key lengths used by today's web browsers are "40-bit" and "128-bit." As a comparison, a 40-bit key can be "cracked" within a few hours by an average personal computer. However, a 128-bit key would take one BILLION powerful computers, each capable of trying one BILLION keys per second. In other words, it would take MILLIONS of years to try every possible combination of bits in a 128-bit key. This type of "crack" or attack is referred to as a brute-force attack and is the only approach that can be used with any secure encryption algorithm.

In the preceding example, the 128-bit encryption is not just three times stronger than 40-bit encryption — it is 309,485,009,821,345,068,724,781,056 times stronger. Performing this same analysis on a 448-bit encryption key yields an encryption strength that is  $2.1 \times 10^{96}$  times stronger than a 128-bit key.

- The speed of the algorithm was also a major determining factor. Some may think a 448 bit key length to be excessive. However, when we analyze the effective throughput of the Blowfish algorithm, we see that even large key lengths result in much faster performance than other encryption algorithms as indicated in the following table:

<b>Speed Comparisons of Block Ciphers</b>				
<b>Algorithm</b>	<b>Clock cycles per round</b>	<b># of rounds</b>	<b># of clock cycles per byte encrypted</b>	<b>Notes</b>
Blowfish	9	16	18	Free, Not patented
Khufu/Khafre	5	32	20	Patented by Xerox
RC5	12	16	23	Patented by RSA Data Security
DES	18	16	45	56-bit key
IDEA	50	8	50	Patented by Ascom-Systec
Triple-DES	18	48	108	

Many factors must be considered when incorporating encryption in any “security-based” software product like NovaNet-WEB. However, encryption speed, key strength and extensive peer review of the encryption algorithm were the key motivating factors behind NovaStor’s decision to utilize Blowfish in our NovaNet-WEB product.

As encryption algorithms evolve to meet the ever-increasing speed of systems designed to “crack” them, NovaStor will strive to incorporate these enhanced algorithms in all of our products.

However, Blowfish will offer substantial security for many years to come and will continue to be the preferred encryption algorithm used by many corporations and banking institutions worldwide.