SecurEnvoy

White Paper

SecurEnvoy Passcode Number Generation

Author: Andrew Kemshall

Date: April 2004

Random Number Generation

SecurEnvoy does not utilise pseudo random numbers to generate it's passcodes as these types of numbers are only as secure as the underlining cryptographic algorithm. As with all algorithms, it is merely a matter of time and processing power before they are compromised. Instead, SecurEnvoy utilise a FIPS-140 compliant random numbers generated via Microsoft's CryptoAPI. At the heart of this API is RSA's BSafe toolkit which most public key private key applications rely on. This toolkit generates the random numbers needed to create the initial key pairs of many of the worlds PKI based application. The BSafe toolkit is a well known and respected method for high quality random number generation.

In addition, modern Intel chipsets (8xx) have built in hardware random number generators that measure the thermal noise of a resistor. This number generator is accessed via the BSafe toolkit and thus is used by SecurEnvoy.

Random Number Testing

In order to undermine a token based pseudo random number algorithm, a skilled cryptographer would generate thousands of numbers and look for any unusual patterns that may lead to predictability.

SecurEnvoy have tested it's true random number generator with 6 million numbers as follows.
A test program was created that generates 1,000,000 6 digit passcodes. Each digit was counted to see if any one number has an abnormally high occurrence which may indicate that some level of predictability is available. The results from this test are shown below:-

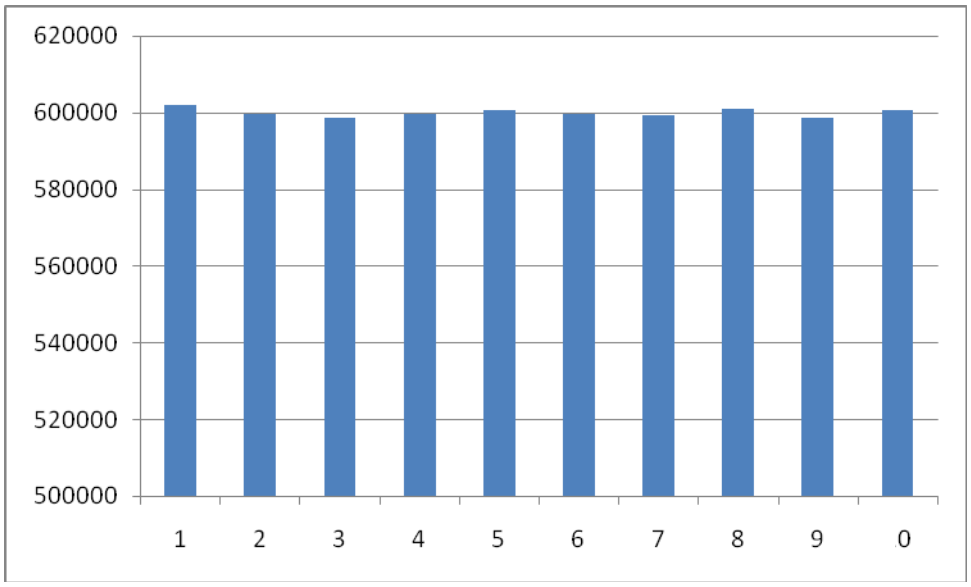
The CPU use for this test is a standard Intel Centrino 1.67Ghz (Core Duo)

1,000,000 * 6 digit passcodes generated (6 million numbers in all)

Number of digits counted
1 = 601990
2 = 599790
3 = 598581
4 = 599693
5 = 600675
6 = 599703
7 = 599266
8 = 600928
9 = 598734
0 = 600646

Lowest Number = (3) 598581
Highest Number = (1) 601990
Difference is only 3409 which is less than 0.0005% over 6 million digits

Number Distribution



Conclusion

Using statistics one would expect a standard deviation of *6000000*/(10).
The maximum deviation measured was less that 0.0005%.
This deviation is inline with expected results from a truly high quality random number generator and demonstrates no unusual tendency towards any one number and thus no unusual patterns that may lead to predictability.