Subject: Commands->Get_Random_Int() is of very poor quality
Posted by iRANian on Sun, 12 Aug 2012 19:59:06 GMT
View Forum Message <> Reply to Message

This function is used as the Crates plugin's random number generator, the following code is used for this plugin:

int Rnd = Commands->Get_Random_Int(1,101);

I get the following output with this code (output in spoilers):
```
 for (int i = 0; i < 100; i++)
 {
  int Rnd = Commands->Get_Random_Int(1,101);
  Console_Output("Rnd = %d\n", Rnd);
 }
```

The resulting output is:
Toggle SpoilerRnd = 75
Rnd = 25
Rnd = 69
Rnd = 23
Rnd = 64
Rnd = 78
Rnd = 59
Rnd = 17
Rnd = 10
Rnd = 21
Rnd = 31
Rnd = 15
Rnd = 46
Rnd = 69
Rnd = 82
Rnd = 31
Rnd = 83
Rnd = 87
Rnd = 15
Rnd = 67
Rnd = 41
Rnd = 10
Rnd = 42
Rnd = 11
Rnd = 83
Rnd = 39
Rnd = 28
Rnd = 27
Rnd = 73
Rnd = 99

Rnd = 7
Rnd = 78
Rnd = 48
Rnd = 11
Rnd = 37
Rnd = 63
Rnd = 4
Rnd = 69
Rnd = 42
Rnd = 81
Rnd = 26
Rnd = 69
Rnd = 48
Rnd = 37
Rnd = 11
Rnd = 9
Rnd = 18
Rnd = 85
Rnd = 36
Rnd = 56
Rnd = 64
Rnd = 60
Rnd = 87
Rnd = 44
Rnd = 85
Rnd = 83
Rnd = 63
Rnd = 5
Rnd = 76
Rnd = 61
Rnd = 94
Rnd = 61
Rnd = 42
Rnd = 54
Rnd = 32
Rnd = 35
Rnd = 34
Rnd = 57
Rnd = 14
Rnd = 95
Rnd = 43
Rnd = 51
Rnd = 2
Rnd = 74
Rnd = 80
Rnd = 30
Rnd = 24
Rnd = 23

Rnd = 70
Rnd = 79
Rnd = 56
Rnd = 97
Rnd = 15
Rnd = 46
Rnd = 78
Rnd = 96
Rnd = 25
Rnd = 29
Rnd = 63
Rnd = 15
Rnd = 1
Rnd = 53
Rnd = 89
Rnd = 47
Rnd = 38
Rnd = 35
Rnd = 51
Rnd = 38
Rnd = 95
Rnd = 57

The pattern is very simple, if a number is returned a few calls later a number in a range of less than 10 higher or lower will be returned (seems to average at a range of ~5 higher/lower) around 85-90% of the time.

I reported this issue to Black-Cell in 2005 if I remember correctly and one of the programmers there acknowledged Renegade's random number generator isn't that great.

The result is what you see on SSGM servers with custom crates enabled, you won't see Spy crates for an hour but after someone picks up one in close succession there will be 1-3 other Spy crates. Same with all the other crates but it's the most noticeable with this one as it has such a low probability of showing up.

The random number generator code might be time based, I haven't checked that and I doubt it as I can't see calls to time based code for any of the random number generator classes (quickly scanning over it) and I see them using rand() for stuff like team remix/rebalance.

Subject: Re: Commands->Get_Random_Int() is of very poor quality
Posted by iRANian on Sun, 12 Aug 2012 20:10:53 GMT
View Forum Message <> Reply to Message

replace it with doom 1's random number "generator"!:

/*

```
** m_oldrandom.cpp
** Contains Doom's original random number generator.
**
**---------------------------------------------------------------------------
** Copyright 1993-1996 by id Software, Inc.
** All rights reserved.
**
** Redistribution and use in source and binary forms, with or without
** modification, are permitted provided that the following conditions
** are met:
**
** 1. Redistributions of source code must retain the above copyright
**    notice, this list of conditions and the following disclaimer.
** 2. Redistributions in binary form must reproduce the above copyright
**    notice, this list of conditions and the following disclaimer in the
**    documentation and/or other materials provided with the distribution.
** 3. The name of the author may not be used to endorse or promote products
**    derived from this software without specific prior written permission.
**
** THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
** IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
** OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
** IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
** INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
** NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
** DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
** THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
** (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
** THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
**---------------------------------------------------------------------------
**
*/

static const char rcsid[] = "$Id: m_random.c,v 1.1 1997/02/03 22:45:11 b1 Exp $";


//
// M_Random
// Returns a 0-255 number
//
unsigned char rndtable[256] = {
    0,  8, 109, 220, 222, 241, 149, 107,  75, 248, 254, 140,  16, 66 ,
   74,  21, 211,  47, 80, 242, 154,  27, 205, 128, 161,  89, 77,  36 ,
   95, 110,  85,  48, 212, 140, 211, 249, 22,  79, 200,  50, 28, 188 ,
   52, 140, 202, 120, 68, 145,  62,  70, 184, 190,  91, 197, 152, 224 ,
  149, 104,  25, 178, 252, 182, 202, 182, 141, 197, 4, 81, 181, 242 ,
  145,  42,  39, 227, 156, 198, 225, 193, 219,  93, 122, 175, 249,   0 ,
```

```
  175, 143,  70, 239,  46, 246, 163, 53, 163, 109, 168, 135,  2, 235 ,
  25,  92,  20, 145, 138,  77,  69, 166, 78, 176, 173, 212, 166, 113 ,
  94, 161,  41,  50, 239,  49, 111, 164, 70,  60,  2,  37, 171,  75 ,
  136, 156,  11, 56,  42, 146, 138, 229,  73, 146,  77, 61,  98, 196 ,
  135, 106,  63, 197, 195,  86,  96, 203, 113, 101, 170, 247, 181, 113 ,
  80, 250, 108, 7, 255, 237, 129, 226, 79, 107, 112, 166, 103, 241 ,
  24, 223, 239, 120, 198,  58,  60, 82, 128,  3, 184,  66, 143, 224 ,
  145, 224,  81, 206, 163,  45,  63, 90, 168, 114,  59, 33, 159,  95 ,
  28, 139, 123,  98, 125, 196,  15,  70, 194, 253,  54,  14, 109, 226 ,
  71,  17, 161,  93, 186,  87, 244, 138, 20,  52, 123, 251, 26,  36 ,
  17,  46,  52, 231, 232,  76,  31, 221, 84,  37, 216, 165, 212, 106 ,
  197, 242,  98, 43,  39, 175, 254, 145, 190,  84, 118, 222, 187, 136 ,
  120, 163, 236, 249
};

int  prndindex = 0;

// Which one is deterministic?
int P_Random (void)
{
 prndindex = (prndindex+1)&0xff;
 return rndtable[prndindex];
}

void M_ClearRandom (void)
{
 prndindex = 0;
}
```

Subject: Re: Commands->Get_Random_Int() is of very poor quality
Posted by iRANian on Sun, 12 Aug 2012 21:14:00 GMT
View Forum Message <> Reply to Message

Seems it might be using a look up table internally, Get_Random_Int() calls Random2Class::operator()(void) for the object FreeRandom which in turn uses member data initialized in the Random2Class constructor which calls Random3Class RNG functions to initialize some member data.

There's a check to reset a member variable to 0 if it's higher than 249 in Random2Class::operator()(void) so..

edit: yeah it's using a lookup table

```
int __cdecl Random2Class__Random2Class(int a1, int a2)
{
  signed int v2; // ebx@1
```

```
  int result; // eax@2
  char v4; // [sp+Ch] [bp-14h]@1

 *(_DWORD *)a1 = 0;
 *(_DWORD *)(a1 + 4) = 103;
 Random3Class__Random3Class(&v4, a2, 0);
 v2 = 0;
 do
 {
   result = Random3Class__operator__(&v4);
   *(_DWORD *)(a1 + 4 * v2++ + 8) = result;
 }
 while ( v2 <= 249 );
 return result;
}
```

Subject: Re: Commands->Get_Random_Int() is of very poor quality
Posted by Xpert on Sun, 12 Aug 2012 21:25:03 GMT
View Forum Message <> Reply to Message

Also, crates like DEPOINTS and DEMONEY doesn't work in SSGM 2.0.2 and SSGM 4.0 because if you do something like

int RndGood = Commands->Get_Random_Int(1,2);

The random number will always be "1".

If it was like

int RndGood = Commands->Get_Random_Int(1,3);

Then the result will either be "1" or "2".

I did the above in my crates plugin to get those crates to work.

Subject: Re: Commands->Get_Random_Int() is of very poor quality
Posted by iRANian on Sun, 12 Aug 2012 22:10:28 GMT
View Forum Message <> Reply to Message

Random2Class consists of:

int FirstIndex;

```
int SecondIndex;
int NumberArray[249];
```

The constructor sets FirstIndex to 0, SecondIndex to 103 and fills NumberArray with random numbers from Random3Class::operator().

Random2Class::operator() works like:

```
int Ret = NumberArray[SecondIndex] ^ NumberArray[FirstIndex];
NumberArray[FirstIndex] = Ret;

FirstIndex++;
SecondIndex++;

if (FirstIndex > 249)
{ FirstIndex = 0; }

if (SecondIndex > 249)
{ SecondIndex = 0; }

return Ret;
}
```

And Get_Random_Int() works like:

```
int __cdecl Get_Random_Int(int Low, int High)
{
  RealLow = Low;
  RealHigh = High;
  if ( Low > High )
  {
    RealLow = High;
    RealHigh = Low;
  }
  return RealLow + (Random2Class__operator__(FreeRandom) & 0x7FFFFFFF) % (RealHigh - RealLow);
}
```

Subject: Re: Commands->Get_Random_Int() is of very poor quality
Posted by iRANian on Sun, 12 Aug 2012 22:14:18 GMT
View Forum Message <> Reply to Message

RealLow + (Random2Class__operator__(FreeRandom) & 0x7FFFFFFF) % (RealHigh - RealLow);

if RealLow = 1 and RealHigh = 2 we get

1 + random number % (2 - 1)

Which always returns 1 as anything modulus (2-1) is 0, 0 + 1 = 1.