Warding off the Enemy – RNG Results May Not Always be what they Appear
eGaming Review: March – 2005

Is your Random Number Generator (RNG) really as random as you think it is? It doesn't take a super-genius to predict the outcomes of a poorly designed RNG, and these attackers may be taking away from your bottom line. Worse yet, you may not be able detect that there's a problem by looking at the RNG results alone.

RNG attackers can be divided into two categories: outside and inside. Outside attackers generally have only the public RNG results to make use of to formulate an attack. They will gather game outcome data from your site over an extended period of time, and try to find patterns and biases in the numbers to exploit the games. Inside attackers are a different matter altogether. They have a secret weapon: intimate knowledge of your gaming system. They may have obtained a copy of your source code through illicit means, or may have even contributed to its original development. They can find ways to exploit the games that no outside attacker could ever find. It has been proven that an inside attacker can successfully predict the outcomes of a poorly designed RNG, even if that RNG passes outcome-based testing.

With software-based RNGs, inside attackers will capitalize on their knowledge of any design weaknesses in your system. Improper seeding of the algorithm could give them the opportunity to reverse-engineer the algorithm to determine what the next outcomes will be. A lack of proper background cycling could leave the door wide open for inside attackers to predict every sequential outcome of your games. Even an inadequately large algorithm period could potentially give them the edge they need to profit from your site. With hardware-based RNGs, faults in the interface between hardware and software may cause patterns and biases that are difficult to detect with outcome-based testing alone. An inside attacker could potentially profit from these problems before you can detect their presence and take necessary action.

These dangers do not lie solely in the theoretical realm. Numerous operators from highly regulated jurisdictions have learned all too late that their RNGs have been compromised, and that their game outcomes have been subject to prediction. The direct financial impact of these errors has been considerable, not to mention the tremendous damage resultant from bad publicity.

So the real question is how you ensure that your RNG is sufficiently random. There has been a great deal of debate lately about outcome-based testing vs. objective-based testing. Outcome-based testing looks only at the output of the RNG results, and does nothing to examine the inner workings of the RNG. Although this type of testing is an important step in verifying the randomness of your RNG, it has only the potential to protect you from outside attacks, and therefore cannot be trusted alone. Objective-based testing goes one step further, combining the statistical analysis of outcome-based testing with a methodical inspection of the RNG design and implementation. Objective-based testing need not be invasive and time consuming, and can protect you from all reasonable forms of attack, including those that emanate from inside sources.

Some would argue that RNGs of the imminent future won't have these weaknesses, and will be impervious to all attempts at prediction. It is true that RNGs are becoming increasingly advanced. Such unassailable sources of entropy as radioactivity and atmospheric noise have already been implemented in many RNGs operating today. As technological and physical barriers are systematically overcome, we will see RNGs based on all the more astounding naturally chaotic forces in the universe. Although these new techniques may be no more random than the older and simpler methods, public perception will likely be the deciding factor as to which solution is superior.

Regardless of how fantastic these sources of entropy become, they will always be subject to the limitations of human design. Even the most random source can be implemented incorrectly in an RNG, and reduced once again to a flawed and predictable device, waiting to be exploited by the opportunistic. When it comes to the design and implementation of any RNG, do your homework, get it right, and don't trust outcome-based testing results alone. The best and only assurance will be obtained by combining the statistical analysis of outcome-based testing with the methodical inspection of objective-based testing.

Bio

Mr. Noah Turner is the Chief Technical Officer (CTO) of Technical Systems Testing (TST), an internationally recognized Accredited Testing Facility (ATF) offering evaluation and consultation services for both the land-based (traditional / terrestrial) and Interactive gaming, lottery and Information Technology (IT) industries.

Office: +1 (604) 873-5833
Email: nturner@tstglobal.com

OFFICES:
Vancouver *– Suite #420, 1367 West Broadway, Vancouver, British Columbia, Canada, V6H 4A7 //* ***O:*** *+1 (604) 873-5833 //* ***F:*** *+1 (604) 873-1075*
London *– Swan Centre, Fishers Lane, Chiswick, London, England, United Kingdom, W4 1RX //* ***O:*** *+44 (0)2087 474 956 //* ***F:*** *+44 (0)2087 427 967*
Sydney *– Suite #305 / 306, 30 – 40 Harcourt Parade, Rosebery, New South Wales, Australia, 2018 //* ***O:*** *+61(2) 9700 7023 //* ***F:*** *+61(2) 9700 7024*
Melbourne *– Level 28, 303 Collins Street, Melbourne, Victoria, Australia, 3000 //* ***O:*** *+61 (3) 9678 9095 //* ***F:*** *+61 (2) 9700 7024*
Macau *– Macau Number 39, 17F Central Plaza, 61 Avenida de Almeida Ribeiro, Macau, China //* ***O:*** *+853 8291 3992 //* ***F:*** *+853 8291 3889*