Better Safe than Sorry

InterGaming Magazine: November 2008

Is your Random Number Generator (RNG) really as random as you think it is? It doesn't take a genius to predict the outcomes of an improperly designed or implemented RNG, and attackers may be sapping profits without anyone even knowing about it. 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: external and internal.

External attackers generally have only the live RNG results to sift through and analyse in order to formulate an attack. Generally-speaking, they will gather game outcome data from the games over an elapsed period of time, and try to find patterns and biases in the numbers to exploit them.

Internal attackers are a different matter altogether. They have a secret weapon: intimate knowledge of your gaming machines. They may have obtained a copy of your source code through illicit or malicious means, or may have even contributed to its original development in the first place. They can find ways to exploit the games that no external attacker could ever find.

It has been proven that an internal attacker can successfully predict the outcomes of an improperly designed RNG, even if that RNG passes *outcome-based testing*.

With software-based RNGs, internal attackers will capitalise on their knowledge of any design weaknesses in the gaming machines. Improper *seeding* of the algorithm provides just the opportunity needed 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 internal attackers to predict each sequential outcome of the games. Even an inadequately large algorithm *period* could potentially give them the edge they need to profit from the gaming machines.

With hardware-based RNGs, faults in the interface between hardware and software may cause patterns and biases that are difficult to detect through outcome-based testing alone. An internal attacker could potentially profit from these problems long before anyone may detect their presence and take necessary action.

These dangers do not lie solely in the theoretical realm. Many operators working in highly regulated jurisdictions around the world 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 resulting from the scandalous publicity that tends to follow close behind.

So the real question is how do you ensure that your RNGs are sufficiently random? The answer to that question is testing!

There has been a great deal of debate over the years about outcome-based testing vs. *objective-based* testing. Unfortunately, much of this debate is made more complicated by misunderstandings about the real facts.

Outcome-based testing looks only at the output of the RNG results, and does not examine the inner workings of the RNG. Although this type of testing is a critical element in verifying the randomness of the RNG, it has only the potential to protect from external attacks.

Outcome-based testing is kind of like test-driving a car. Sure, it's a critical step in making the right choice, but it's no substitute for a professional mechanic's inspection.

Objective-based testing goes one step further, combining the statistical analysis of outcome-based testing with an inspection of the RNG design and implementation. Following the same analogy, it's like test-driving a car directly to the mechanic shop, so that they can properly inspect the vehicle for safety and performance.

If performed correctly and methodically by an approved testing authority, objective-based testing need not be overly invasive, time-consuming or costly. The best part is that it can protect your organisation from all reasonable forms of RNG prediction attack, including those that emanate from internal sources.

Although many operators and suppliers choose to have their RNGs tested for their own piece of mind, they also must abide by regulation. Most regulatory bodies mandate that a certain degree of RNG testing be conducted by independent bodies, such as Accredited Testing Facilities (ATFs). Some regulators will require only outcome-based testing, while others are not satisfied until full objective-based testing has been successfully completed.

Whether it's so you can sleep at night knowing that your company's name won't turn up in yet another headline about fraud in the gaming industry, or just to satisfy the requirements set forth by a regulator, RNG testing is a vital step in keeping profits where they belong: in your pocket!

When it comes to the design and implementation of any RNG, spend the time to do some homework, get it right, and get it tested. The best 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*