

The Evolution of RNGs

iGaming Business Magazine: Quarter 1 – 2006

The face of RNGs is changing, and the brain behind the face is changing too. Years ago, gaming operators needed only to worry about attackers predicting the outcomes of their RNG, or other technical exposures of the like. Today, the countermeasures to these exposures are only the minimum requirement for safe and secure operations. The next logical step has come, as gaming operators are now competing for market share with the creativity and marketability of their RNG design.

Over the years, RNG technology has advanced in leaps and bounds. To understand the nature of RNGs today, one must first understand their origin.

The first RNGs were simple physical devices. A pair of dice, or even a coin tossed into the air actually constitutes a Random Number Generator. It was only a matter of time before these physical devices would inspire the invention of mechanical gambling systems, such as the poker machines and slot machines of the late 1800's. The reel stops on these machines were determined by notches on a wheel. Just as dice can be weighted to produce a bias, these wheels could also be biased by filing down the notches.

Over time, skilled players learned tricks to manipulate the spinning reels of these older slot machines to favour preferred outcomes. Magnets, vibration, and even an accurately timed pull of the handle could yield the desired results.

Manufacturers of slot machines were eventually driven to more advanced technologies for their RNGs. There were then, as there remains today, two basic types of RNGs: software and hardware.

At the heart of every software RNG is an algorithm. Software RNGs are also known as pseudo-RNGs because these algorithms generate outcomes that only *appear* to be random. Some would argue that the pseudo-random behaviour of software RNGs makes them inferior. This is a not necessarily correct. When implemented correctly, with proper seeding and background cycling, software RNGs can be sufficiently random to thwart even the most expert and informed attacks. Conversely, when designed poorly, software RNGs can put you out of business.

Hardware RNGs are a whole different ball game. Hardware RNGs are comprised of a physical hardware device, such as an electronic circuit board, coupled with special interface software. Hardware RNGs are capable of truly random output. Since hardware RNGs do not depend on an algorithm, such factors as seeding and background cycling simply do not apply. However, Hardware RNGs are far from perfect. Hardware components can fail, introducing a bias that can be exploited. Consider how component failure on an electronic circuit board can introduce bias. This is analogous to a roulette wheel that is off balance.

This leads us to the latest evolution in Hardware RNG's, where numbers are based on taking samples of external random events.

This is where things get interesting. External random events can be found almost anywhere, from the smallest atomic particles to the vastness of time and space.

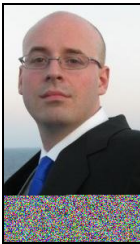
Hardware RNGs are using increasingly advanced sources of external random events. Such unassailable sources of entropy as radioactive decay and atmospheric noise have already been utilized successfully in many Hardware RNGs operating today.

As technological and physical barriers are systematically overcome, we will see RNGs based on all the more astounding forces of natural chaos in the universe. An Environmental RNG[®] developed by Sky² uses events such as solar flares and the Aurora Borealis. Although these new techniques may produce outcomes that are no more random than properly implemented traditional methods, public perceptions often favour reality over the abstract.

It is easy to see that many players will be drawn to gaming websites that advertise such amazing sources for their random numbers. Furthermore, by coupling the source of random numbers with the overall theme of the website, gaming operators can rope in players that are inherently attracted to their particular theme.

When it comes to the bottom line, more players means more profits. So next time you're faced with a decision about what RNG to implement on your new site, remember that a little creativity could go a long way... straight to the bank!

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