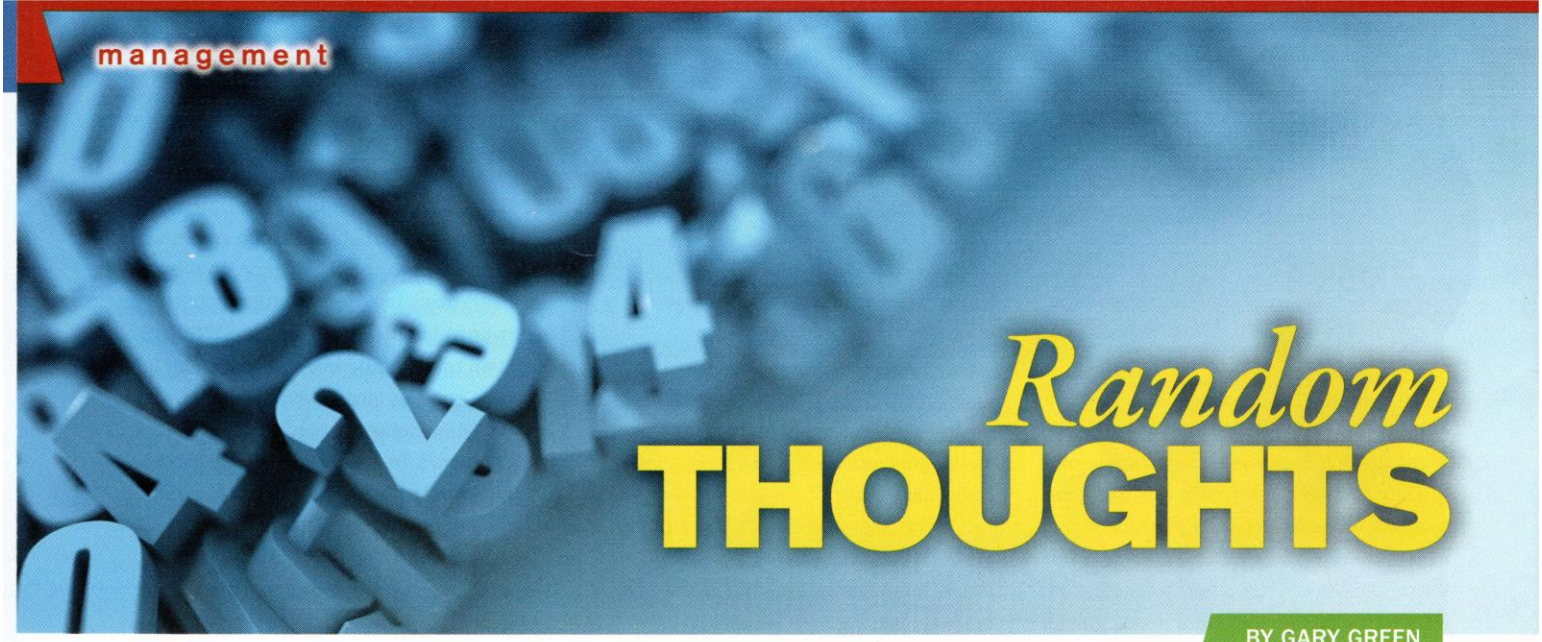


Random THOUGHTS

BY GARY GREEN

Random number generators (RNGs) in certain older models of slot machines are vulnerable to hackers, but there are steps operators can take to better protect against this crime

Our industry has a dirty little secret that is "secret" to almost no one inside gaming, but is so surreptitious to players that a Federal Court sealed the records of a case revealing the details. It took a February 2017 article in Wired magazine to give non-insiders the knowledge that slot machine random number generators are ... well, not so random.

"Ha-ha; old news," said Bradley L. Wilson, longtime slot company executive and former director of analytics for the very successful Best Sunshine Casino in Saipan. "For a very long time, game developers have known games do not use a true RNG. This issue has long been debated by developers."

That old debate resurfaced in mid-March when the *Las Vegas Review Journal* reported that Russian hackers were again exploiting the industry-secret, this time in South America. According to Rex Carlson, the former lab manager for the Nevada Gaming Control Board, there has been a syndicate of Russian hackers using the secret and syphoning cash from U.S. casinos for the past decade. In fact, in 2014 the FBI and Homeland Security brought Federal indictments against four Russian nationals, charging that they conspired to cheat at least 10 casinos in Missouri, California and Illinois. The details of those indictments and how the hacks took place is what a judge for the United States District Court for the Eastern District of Missouri sealed from public view.

Speaking at this year's World Game Protection Conference, Carlson warned regulators and operators that the supposed randomness of some slot machine random number generators in fact can be, and have been, defeated to the tune of millions of dollars.

Of course, Brad Wilson was right about it being old news. The bible-esque *Practical Casino Math* textbook, written by guru statistician Dr. Robert Hannum and Vegas attorney Tony Cabot, clearly points out that, "the RNG produces pseudo-random numbers that act like random numbers." Even the widely-implemented "GLI-11" regulatory standards tacitly warn that without certain technological precautions, it absolutely is feasible to predict future RNG outcomes.

WHY IS OLD NEWS NOW NEW?

With 68 percent of American adults carrying in their pockets a smartphone with more computing power than was onboard any of the Apollo space missions, we have all become much morehack-aware, if not hack-savvy. Plus, with the last election's revelations and questions about hacking servers, we are once again Russia-wary.

With pocket-computing rampant, attention to vulnerabilities is not only prudent but absolutely necessary. A Ponemon Institute study for *CNN* claims that 432-million Americans—47 percent of the adult population—were hacked last year. IBM's 2016 Cost of Data Breach Study reported that data breaches cost companies an average of $221 per compromised record and the cyber security market is projected to be worth $202.36 billion within the next five years.

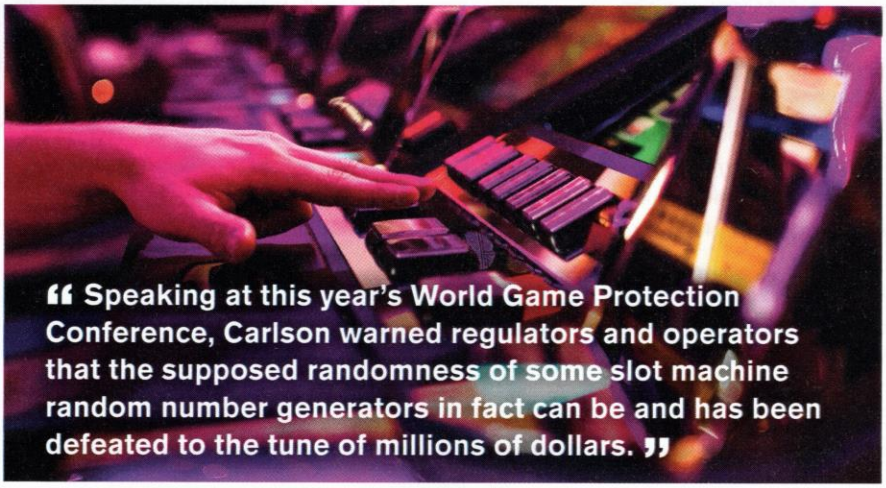
The FBI has an entire Cyber Crime division with its own assistant director; and newly-declassified documents show that U.S. investigators suspect that Russian intelligence services have access to compromised computer infrastructure in as many as 60 countries.

A study by the Business Software Alliance revealed that 89 percent of the software in Russia today is hacked software, and Carney Forensics reports that the majority of the hacking of American-based systems is from either Russia or former Soviet Republics.

In early 2014 a former NSA director called China's hacks into American computer systems "the biggest

transfer of wealth in modern history;" but in September of 2014 Chinese President Xi Jinping signed a treaty with the U.S. to halt the breaches. Russia has signed no such agreement and according to Foundstone (the cybersecurity company that owns McAfee anti-virus), Russian hackers are even more focused on direct financial crime.

Between the hacked medical records of Serena Williams and Simone Biles, the Democratic National Committee's server, and Hillary Clinton's e-mails, public awareness of Russian hacking is clearly heightened; so the old news about Russians hacking slot machines is certainly topical today.



"Speaking at this year's World Game Protection Conference, Carlson warned regulators and operators that the supposed randomness of some slot machine random number generators in fact can be and has been defeated to the tune of millions of dollars."

IT'S PUTIN'S FAULT

At the height of his 2009 crackdown on the Georgian Mafia, Russia President Vladimir Putin ordered a sudden middle-of-the-night permanent closing of Russia's 550 slot rooms and 30 casinos. This left the operators with a glut of owned slot machines and nothing to do with them; suddenly several thousand slots were for sale for bargain-basement prices. As we all know, the slot machine industry is an international business, so the machines being sold were the same games that are familiar to operators all over the world.

Among the buyers scooping up those well-known games for next-to-nothing were a few collectors, some American and Caribbean reseller companies, and a handful of unscrupulous entrepreneurs who simply copied the chip-embedded game programs to sell knock-offs at a fraction of the price of the real product. Four of the titles were bought by a St. Petersburg computer geek who just wanted to understand how jackpots payout. Unknown to him, his curiosity revolved around the dirty little secret.

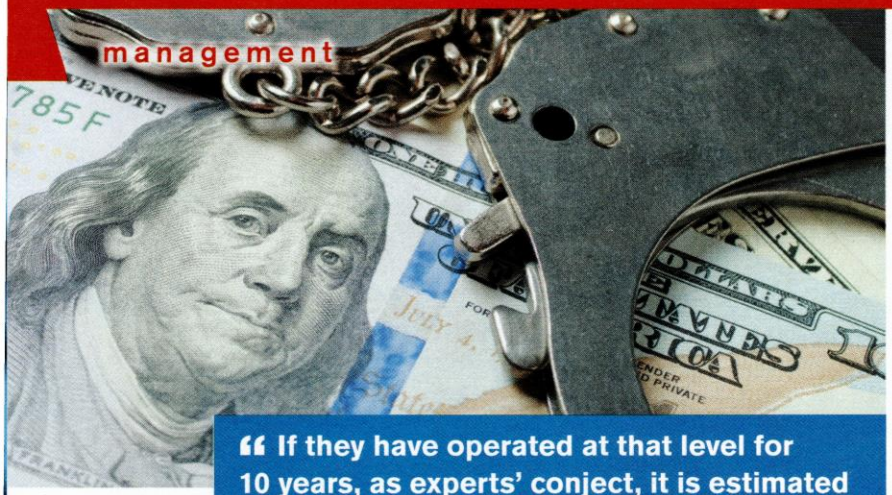
As early as 1979, in Atlantic City, I was naively asking, "If a slot machine win is truly random, how is it possible that there is not the same chance of winning the top jackpot as there is of winning an even-money 'one cherry' spin of the reels?" Driven by basically the same question, the St. Petersburg technologist had purchased the games to find the answer.

In relatively short order, he had advanced far beyond such neophyte musings about "random within certain parameters" to a technical analysis of how the games' algorithms generated a sequence of numbers that mimicked actual random numbers. As a technologist, he realized that the supposed RNG was actually something called a "deterministic random bit generator," a pseudo random number generator, or PRNG.

If that was the case (and it was), then the outcome of a game had to be completely determined from a relatively simple and trackable starting point; that starting point was the frequency and size of payouts. If he could determine that "seed value" of the computer program, then he could predict what "random number" the slot machine would generate. In short, he could determine when the game would payout and when it would not.

He had purchased four different games and created by four major international slot machine companies. After playing thousands of times on those four games, he realized that it was not so simple after all. The programming source code for those "seed values" also contained another number that was constantly changing as long as electricity was running to the slot machine's computer. This new number was determined by the ticking of the internal clock of the computer controlling the game. A clock-generated variable changed every fraction of a second as the clock itself changed.

While theoretically it was still possible



> **“ If they have operated at that level for 10 years, as experts’ conject, it is estimated they have made $9 billion from the scam. ”**

to predict the outcome, the number of possibilities was impossible for the human brain to fathom. Just listing all the possibilities would require massive computing power. Finding patterns within those possibilities should have been impossible; and our industry counts on that impossibility. With enough computing power however, the clock timer could be matched to the huge number of possible outcomes. With even more computer power, whatever was appearing on the video screen at any given time could be matched to the results from the possible outcomes and the clock timer.

That is where our dirty little secret comes out. The game outcome is not random at all; it is highly structured and follows a specific pattern. It works for us in the industry because the number of possible patterns on a simple 25-line video slot might as well be random since there are about 259.4 million possible patterns. Within that range, the number might as well be random—it is certainly unpredictable by any human brain.

The St. Petersburg technician, however, had a lot of computing power at his disposal. In fact, he was able to not only run all of the possibilities and match them to the internal clock, but he was able to match that data to what was happening on the video screen at the same time. Depending what was showing on the screen at any given time, he could predict the outcome of the game.

Had Putin not closed down those casinos, this breakthrough could have never happened and our secret would have been safe.

HOW THE SCAM WORKS

He had the tools to determine the outcome of four games. If he could find a way to make that determination portable then he could travel around the world to any casino that had those four games and make a fortune. And he did just that.

First, he would send someone into a casino to determine if the right games were on the floor. If they were there, the next step would be to return to the game with two cell phones. The first phone would be in a shirt pocket with a gauze peep-hole to send a video of the slot machine screen back to Russia via Skype or another video conferencing app. That video would be run in real time against the data assembled for the game. In a very short sequence of 24 spins, the computer in Russia could determine the internal clock sequence of the slot machine at the casino by matching the video screen to the data about that game.

The player had a second cell phone in a pants pocket. One-quarter of a second before the Russian computer determined a payout was eminent, the computer would send a vibration to the second phone. That quarter-second was long enough for the customer to hit the play button on the machine in time to win the game.

To avoid detection, the player would put $20 into a machine, win less than the mandatory $1,200 W2-G amount, and move on to another machine. A typical player could win about $250,000 a week using this technique for about 30 wins a day. The player was allowed to keep 10 percent of that; a regional manager got another 5 percent and 85 percent went home to mother Russia and our little computer technician ensconced safely in St. Petersburg.

A team of between 40 and 70 operatives, each generating about $250,000 a week, has kept this up for almost 10 years. They have only been caught twice—one arrest at a Southern California casino after they were recognized from a Missouri all-points bulletin; and once in Singapore.

If they have operated at that level for 10 years, as experts’ conject, it is estimated they have made $9 billion from the scam.

WHAT CAN BE DONE

In my television series, *Casino Rescue*, one of the first things I do is visit a casino “undercover” to evaluate the slot floor. Among the many things I look at are the types of games, regardless of manufacturer.

First, and most importantly, I look for games with a “cryptographic” RNG; these are programs specifically designed to use a starting point other than the machine clock and to have that starting point constantly changing in a disorderly near-entropic manner and periodically changing their method for setting that starting point. Whether or not the jurisdiction’s regulatory authority requires this step, I do.

Next I look for the number of possible outcomes from the par-sheet. While those older Russian-studied games have a little more than a quarter-billion possible outcomes, many of the newer games have 552 septillion outcomes. That is 552 times 1024. Since the secret is out, and part of the success of the PRNG is the number of possible outcomes, I consider “the more outcomes, the merrier.”

Another solution: out with the old games, in with the new. Unfortunately, a lot of those older games are player favorites that casinos are reluctant to give up. But from a security standpoint, it would probably be best to decommission those older games.

So yes, our industry has a dirty little slot machine secret; but we’ve got it covered... if we are diligent. **SM&M**

Gary Green *is a longtime industry observer, slot manufacturer executive and casino developer. He is the host of the new television series Casino Rescue and is chairman of the casino private equity holding company Gary Green Gaming. He can be reached at www.garygreengaming.com.*