Lottery Insider, Vol. 78, no.5, January 2016

Author: Helena Pereira, Szrek2Solutions

Title: RNG Integrity: Perceptions of Fraud Risk and Known Vulnerabilities

Article:

The growing potential threat of RNG fraud has raised many questions. These begin with practical questions that lotteries should ask themselves such as "what are the real vulnerabilities of an RNG system?" to questions about what the possible consequences could be of an attack. Would RNG fraud only affect the lottery in which it occurred or would other lotteries also be negatively affected? Who in the end is responsible for avoiding or preventing such attacks? I address both the technical and practical question of what the vulnerabilities are by reviewing different known vectors of attack to the RNG system. I then discuss industry perceptions of RNG fraud through a survey conducted at NASPL in October 2016.

The vulnerabilities of a traditional RNG system

Traditional RNG security is built around protective security. This type of security has been consistently increasing in most lotteries and RNG vendors have updated their protective security measures. Such measures include background checks of all personnel, the use of only verified vendors, the creation of a secure environment with restricted access, the development of security procedures, role separation for the draw staff, digital signing of draw reports, certification, and code review, etc. In addition, in some locations – including in most US states – RNG machines are designed to be on an isolated system that is not connected to a gaming system. However, even when the RNG is isolated it can be vulnerable to insider attacks, and insider attacks make up the large majority of security breaches across most industries (Kroll, 2015).

We refer to traditional RNGs as RNGs that have protective security, as described above, and limited detection capabilities. We note that not all traditional RNGs are alike, and there may be additional security measures used to enhance security. However, unless the vendor offers all-encompassing fraud detection *and* verification independent of a potentially defrauded RNG system, the RNG system will be vulnerable to the following vectors of attack, by insiders who have access to the system, be it lottery personnel, the RNG provider, the certification authority, etc.:

- *The possibility of fraudulent software being substituted on the certified RNG for a specific draw*: We are currently aware of two such methods of attack, (i) hidden code or a dynamic link library (dll) can be installed on the RNG system at the time when the original code is installed or at a later time, and may be triggered by a specific date or event, (ii) a self-destructive root-kit can be installed on the RNG system at the time of original installation or afterwards, e.g. at a time of system maintenance. In all cases, such software may be very difficult or even impossible to detect because it can be hidden, encrypted, self-destructive, and because it may only run at a specific time. Methods such as certification may not detect such hidden code because it runs only at certain times or is dependent on other conditional factors related to number generation. Pre and post-testing of draws will not detect the hidden code because such tests focus on analyzing statistical distributions. Verification of program checksums may fail because a different program may be running than the check-summed one or because a verification tool may be corrupt. Scanning of the system may not identify such falsified code – it is very difficult to find something suspicious in a vast amount of code unless you are looking for a specific type of attack. Verification tests cannot find hidden code because they can only test for known problems and cannot predetermine all potential vectors of attack. For example, in a recent RNG fraud case, fraudulent software was only detected after the fact, when it was already known that there had to be fraudulent software that was used on a specific date. As attackers are improving their methods, it will become more and more difficult to detect fraudulent software.

- *The possibility of fraudulent hardware substituting the RNG hardware for a specific draw*: Unless there is a way to identify which hardware was used through background cycling, the substitution of hardware can go unnoticed.

- *The possibility of the time of the draw being altered*: In an offline or isolated system, the system time cannot be continuously verified. This means that the time of a draw could be altered to after the draw results are known by an insider.

- *The possibility of phishing for desired combinations:* A traditional RNG, and in particular an offline system, may allow for multiple generations of draw results. This would allow an insider to continue phishing until a desired draw result is found. This desired draw result could then be published as the proper draw outcome.

- *The possibility of hardware deteriorating and the RNG not functioning properly*: RNG hardware may deteriorate over time leading to such problems as a non-random draw. Faulty hardware may still generate numbers but their properties may not be random and it would not be known that there is a problem.

Perceptions of RNG fraud vulnerability and responsibility

Should we be worried about RNG fraud? Are there any consequences of RNG fraud to the industry? In an earlier survey, we questioned lottery directors and top management from the lottery industry about the consequences of RNG fraud. We learned that top managers in the industry believe that RNG fraud would lead to customers purchasing fewer tickets and lotteries losing legislative and regulatory powers (such as the ability to develop new games); we also obtained some preliminary estimates for the costs of fraud in the short and long-term (Pereira, 2016). In this current survey, we asked respondents from different roles in the industry, to give us their view on the impact of another lottery fraud on the industry, if it occurred. To test the hypothesis that this impact was independent of the size of the fraud, we asked about RNG fraud involving larger (greater than $1 million) and smaller (less than $500) amounts of money. We also asked respondents how much an RNG fraud discovered in one lottery would negatively affect other lotteries. Finally, we asked respondents to identify the different entities that should be held responsible for lottery fraud.

Results

There were 56 respondents in total, 27 of which were from lotteries, 12 from vendors that sell gaming systems, and 17 from other vendors (consultants, audit, etc.). Fifteen of the 56 respondents were lottery directors (see Table 1).

Table 1: Respondents' roles in the industry (n=56)

Lottery (n=27)	(15 Lottery directors, 10 top management, 2 middle management)
Gaming Vendors (n=12)	(1 CEO, 8 top management, 3 middle management)
Other Vendors (n=17)	(6 CEO, 8 top management, 3 middle management)

We found that respondents expected a RNG fraud of 1 million dollars to be a 7.8 on a scale of 0 (no impact on the industry) to 10 (complete shutdown of the industry), with 84.5% of responses a 7 or above and all but one response above 4. However, when the dollar amount was $500, the mean response dropped to 4.84. Although, 27% of respondents showed no change in their response when the dollar amount dropped, 23% of respondents showed a drop in 4 points or more. Respondents informally described their answers in terms of how the dollar amount would affect the interest of the story to the press. In terms of how a fraud in one lottery would affect other lotteries, respondents on average thought this would have an effect of 5.93, on a scale where 0 is that the fraud would only affect the lottery in which the fraud was discovered and 10 is that the fraud would affect all lotteries in the industry. 55% thought the effect would be between 3 and 6 and 39 % of respondents thought that the effect would be 7 or above. See Table 2 for mean responses to all survey questions.

Table 2: Mean responses of survey questions

	FULL SAMPLE (n=56)	
Variable	Mean	Std. Dev.
How bad would another RNG fraud incident be to the lottery industry if the fraud involved a large amount of money (ex. over $1million), where 0 is that it would have no effect at all and 10 is that it would be utterly devastating to the industry.	7.77	1.82
How bad would another RNG fraud incident be to the lottery industry if the fraud involved a small amount of money (ex. less than $500), where 0 is that it would have no effect at all and 10 is that it would be utterly devastating to the industry.	4.84	2.81
How much do you think a fraud incident in one lottery would negatively affect other lotteries, where 0 is that the fraud would only affect the lottery in which the fraud was discovered and 10 is that the fraud would affect all lotteries in the industry?	5.93	2.55
Who is responsible for preventing RNG fraud?		
Lotteries	1.00	0.00
Vendors of Gaming Systems	0.73	0.45
RNG suppliers	0.79	0.41
Certification authority	0.63	0.49
AUDIT/ICS provider	0.48	0.50
Legislature/Govt	0.30	0.46
Regulator	0.41	0.50

Respondents always held lotteries responsible for RNG fraud, while the other entities were held responsible by some but not all respondents, Vendors of Gaming Systems (73%), RNG suppliers (79%), Certification authorities (63%), AUDIT/ICS providers (48%), Legislature/Government (30%), and Regulators (41%). Respondents generally had different reactions to this question; some believed in one entity (lotteries) having sole responsibility while others considered RNG fraud to be an issue whose responsibility should be shared across the different entities.

Although there were differences in the responses across type of respondent, the differences were not statistically significant except in two cases. Mean responses to the first question (how bad another RNG fraud would be to the industry, $1million or above) were highest in the gaming vendors (8.58) compared to other vendors (6.94), with lotteries in between (7.93). Mean responses to the second question were statistically different between lotteries (5.33) and other vendors (3.65) but not gaming vendors (5.42). Lottery directors on average (n=15) had responses that were very close to the mean of the sample, with means to the first three questions at 7.87, 4.93, 5.53. All in all, the responses suggest that RNG fraud would have a large effect on the lottery industry, consistent with our earlier study.

Discussion

RNG fraud is more than just a potential threat. Rather than discuss the topic solely behind closed doors, open discourse on RNG fraud may assist by bringing people together to develop ways to avoid, mitigate, or detect fraud.

Similarly, by openly surveying industry opinion about RNG fraud, we can raise awareness about different problems and begin to develop solutions. In particular, the current survey results suggest that the industry perceives the threat of a new fraud case to be consequential to the industry, and even to have systemic consequences. Because of this, it is important that the industry develops means of building trust and integrity around the use of RNGs, hence seizing all the enormous benefits of the adoption of this technology while minimizing its risks.

Currently, there are two complementary ways of addressing this challenge: first, by increasing preventive measures; and, second, through robust proof of the integrity of draws that can be independently audited. Preventive measures can be systematically incorporated into processes and best practices so that the likelihood of success of any attack is reduced; however the main disadvantage of preventive measures is that they can only address known vectors of attack and with cybercrime becoming more ubiquitous this may be insufficient. Second, through true proof of integrity, lotteries can unequivocally demonstrate the validity of each and every draw, can detect fraud when it occurs, and can prosecute offenders should it occur. Furthermore, complete proof of integrity, by eliminating the benefits of engaging in such crime, will have the added benefit of working as a fraud deterrent. However, if proof of integrity is not complete and if there are ways to erase traces and avoid detection, such deception methods will be discovered by those with the right (or wrong) incentives.

The industry should rely on both preventive measures and true proof of integrity to build trust around its activities. I hope that we can create more opportunities to discuss RNG fraud openly so that we can begin to solve these issues together as an industry.

References:

Kroll. (2015). *Global Fraud Report 2015/2016*, November. Available from: http://www.kroll.com/en-us/intelligence-center/press-releases/the-threat-within-insider-fraud-on-the-rise.

Pereira, Helena. (2016.) *The Importance of Security and Fraud Detection for Electronic Drawings. Public Gaming International*, July/August pgs. 54-55. Available from:http://www.publicgaming.com/PGIJULYAUGUST2016/PublicGamingMagazineJuly-August2016/HTML/#54.