Szrek2Solutions

The Importance of Security and Fraud Detection for Electronic Drawings

By Helena Pereira, PhD, Marketing Director, Szrek2Solutions

SHORT SUMMARY

Electronic draw systems based on RNG have become an integral part of the lottery industry and require utmost security to reduce exposure to potential fraud. Insider fraud, where an employee of the lottery, an operator, or vendor, takes advantage of their system knowledge and access to the system to fix a draw outcome, is the most dangerous and difficult to detect. There are existing security methods that can protect lotteries against such fraud.

INTRODUCTION

Lottery drawings using electronic random number generators are integral to the future of modern lotteries. Lottery industry leaders have recognized that they must embrace electronic drawings: while offering potential for growth, electronic drawings also offer major cost savings to lotteries.

However, lotteries worry about potential fraud with the shift from mechanical to electronic drawings. In a recent lottery fraud in the US, the perpetrator was seized by coincidence, which raises the question of how many other fraud cases were not detected.

In this article we discuss the costs of fraud and the probability of RNG fraud in the US, and we provide some guidelines for RNG security.

THE COSTS OF FRAUD

At the recent Public Gaming conference, we approached top-level lottery management to obtain their perceptions of fraud in the lottery industry *(see Table 1)*. The survey results suggest that fraud would be damaging to lotteries by reducing their customers, restricting lottery's freedoms to introduce new products, and through imposing large monetary costs on lotteries in the short and medium-run. The average estimates of fraud cost to their lottery provided by lottery leaders was $283 Million, for the first year, and $1.31 Billion, for years 2 to 5 after the fraud occurred. The survey did not take into account other potential impact such as increased financial risk of liability through class action, so the numbers may be understated. These numbers are also based on a survey rather than actual costs that were measured, so they are only suggestive. However, they highlight that lottery managements believe fraud could severely affect their institutions in many ways. To avoid this impact, the best safety and security procedures should be introduced to protect lottery systems and particularly electronic draw systems.

THE PROBABILITY OF RNG FRAUD

With large potential winnings, insider fraud is a true threat to the lottery industry. In the US, many lotteries have been victims of fraud in the electronic drawings for games played within or across states. *Currently we can estimate that over the last 5 to 10 years electronic draw fraud has occurred in games played across 13 states. If all 50 states used electronic draw systems, this would put the probability of electronic draw fraud at 26%.* This underestimates the amount of fraud, because some states do not take part in electronic draws, and we can only report the amount of fraud that has been discovered and reported.

SECURITY MISCONCEPTIONS

Misconception 1: Mechanical drawing machines are more secure.

Explanation: With high potential costs and prevalence of fraud, one approach would be to return to mechanical machines. However, when the security measures are correctly implemented, an electronic draw system allows the lottery to control and protect the gaming environment better than with a mechanical system, making the electronic draw system also more secure than a mechanical system. Ad-

Table 1: LOTTERY FRAUD SURVEY RESULTS

In a survey of 9 lottery directors, 2 former directors, 1 CFO, 1 COO, and 6 other top level management (n=19):

- On average, respondents thought that over half of their customers may stop purchasing lottery tickets or buy fewer tickets if they discovered that lottery fraud had been committed in that state.
- Lottery's legislative and regulatory powers, including the lotteries ability to develop new games, would be impacted by the discovery of lottery fraud—95% agreed.
- The total short-run costs estimated were, on average, $283 Million for the first year in which lottery fraud was detected. Total costs include reputational costs, legal fees, political costs, losses in ticket sales, etc.
- The total medium-run costs estimated were, on average, 1.31 Billion for the first 5 years in which lottery fraud was detected. Total costs include reputational costs, legal fees, political costs, losses in ticket sales, etc.

ditionally, electronic draw systems offer more capabilities, such as the support for more types of games, the ability to have more frequent draws, and the capability to manage draw outcomes. Such systems are also much less costly because the games can all reside on one system and require much less human involvement to manage them.

Misconception 2: Electronic draw systems are most secure when they are isolated from other systems or networks and protected using physical measures.

Explanation: Isolating draw systems does not protect from insider attacks, as demonstrated by the recently discovered fraud cases. Additionally, committing to stand-alone offline draw systems introduce limitations on draw capabilities which may limit lottery growth and require manual procedures that are more prone to error than automated ways of communicating data; they require more human effort, and have higher operational costs.

WHAT SECURITY MEASURES ARE PROVIDED BY RNG VENDORS?

To provide some guidance, we identify a checklist of 7 critical security measures which help protect the integrity of the RNG. (1) –(5) are elements that improve on traditional methods of assuring integrity and are best practices provided by third-party vendors. Fraud detection and independent verification, (6) and (7), are deployed by some lotteries for enhanced security.

1 Draw systems should be provided by an independent third party. To avoid potential conflict of interest: (a) lotteries should not develop their own draw systems and (b) lottery gaming systems vendors should not provide their own draw systems.

2 Security of the RNG must include state-of-the-art protective security which should include: strong password protection, restrictions on access, and read-only use of the RNG program, configurations, and reports. Also, lotteries should set procedures to restrict user access and define role separation, including users from different groups or organizations to perform draw, audit and other functions.

3 Independent certification of randomness and code review is necessary. This certification may not detect a hidden code or prevent injection of fraudulent code in the future.

4 Another important method requires verification of RNG software code checksums, or hashes, to detect any changes in code or configuration since certification. This verification may be circumvented by a fraudulent software.

5 Additional security certifications can be performed to increase confidence in the system. These certifications may include scanning of the RNG system delivered to the lottery to detect malicious code and system vulnerabilities. A system snapshot can be taken at the time of delivery and used later for comparison to detect unauthorized changes.

6 The RNG includes fraud-detection capabilities: each time a draw occurs, the system creates a tamperproof log file corresponding to the draw; if any changes are made to the log file, an independent audit would identify these changes. By building a tamperproof log file, the draw provides non-refutable/undeniable proof of draw integrity. To clarify the principle of logs and audit:

   a. If log files are not tamperproof, fraud-detection is not certain.

   b. A tamperproof electronic log file is distinct from activity log and draw reports; computerized attacks may be 'invisible' and they may create fraudulent logs.

   c. Proof of integrity of a draw system should not require sharing of privileged or secret information, as this can involve potential collusion and fraud.

   d. Digitally signing already generated data does not provide undeniable proof, as the data may have already been modified when signed. In fact, draw reports generated in the recently publicized RNG fraud case were digitally signed.

7 A draw system should be accompanied by an independent audit system. The audit system must be independent from the number generation process, so that it can detect any fraud to the draw system.

   a. Audit system should be able to analyze tamperproof logs (6) to prove the integrity of each individual draw, its time and numbers drawn.

   b. Audit should not rely solely on scanning of draw systems as these procedures are not fully reliable: some evidence may not be recoverable through the scans. A skilled programmer will not leave traces of attack or make them extremely difficult to find.

CONCLUSION

We recommend that lottery directors and top management understand how alternative RNG solutions solve various security risks including insider fraud. We provide some guidelines in identifying a secure RNG solution. We also recommend that when choosing a RNG system, lotteries make a broad cost analysis that takes into account the level of RNG security offered, whether fraud detection is included, and how these factors impact fraud susceptibility. Lotteries can obtain impartial comparative analysis of different offerings from third party experts, familiar with the technology used and without financial interest in selling or promoting specific RNG solutions. Our hope is that in the future the industry will help lotteries by regulating RNG security, but in the meantime lotteries need to fully understand the security risks for RNG products offered.

The recent fraud in the US illustrates many of the points we discuss: the security solution of the defrauded RNG was stronger than that of RNG solutions used currently by many lotteries. It is alleged that the fraudulent code was designed to only run at a specific time and date—at the actual draw time. It is hard to defend against such an attack, as this dynamic code may reside outside of the RNG code, could be replaced by a script running in the background, and could even erase all traces of fraud after running. The investigators deserve credit for detecting this fraud. It may have gone undetected, as we suspect can be the case for other fraudulent events. Right now, this should alert us all to the potential of RNG fraud and to finding a reliable solution for detecting fraud. ■