Drawing Machine Compromised (?)

Eddie Tipton, Security Director of MUSL, was arrested in January 2015 and charged with fraud related to a Hot Lotto ticket he purchased in 2010. This ticket won over $10.8 million in cash, with the odds less than one to 29 million. Coincidentally MUSL carries out lottery drawings for Hot Lotto and other games on a random number generator (RNG) developed in-house.

When a security director of a lottery organization running a RNG draw wins a multimillion jackpot prize, it likely raises speculation that the draw was rigged. An insider with access to the draw system and internal information is able to circumvent security procedures, and ultimately fix the draw. In such situations, when security of the RNG relies on preventive security procedures that can be bypassed, it may not be possible to unequivocally prove whether the draw was fixed or not. Considering that integrity is essential to the lottery industry, it is very important to prove if a draw process was compromised and to avoid any speculations about process integrity.

Typical Random Number Generator

A typical approach to RNG based lottery drawings is to rely on RNG certification and preventive security measures: the RNG gets tested and approved by an independent lab, the computer generating random numbers gets secured and placed in a protected environment, and security procedures for running the draw get established. As long as all these protocols are followed the draw process is secure. However if the draw computer was compromised, then the RNG outcomes could be manipulated and traces of the fraud removed. An insider with internal system knowledge and access to the draw system can circumvent the security procedures, change the draw outcome to his/her advantage and eliminate any traces of these actions. Standard audit will not work if an attacker gains privileged access to RNG system. This is because standard audit procedures rely on integrity of information on RNG systems, such as logs, access controls, file privileges, which would be attacked, so cannot be trusted.

Obviously this approach can create major problems and to eradicate them lotteries should turn to RNG technology which does not rely on honesty of staff for secure generation of random numbers.

Auditable Random Number Generator with Fraud Detection

Auditable RNG technology was introduced by Szrek2Solutions in 2004 and has since been used by several lotteries[1] - it allows for irrevocable determination regarding whether the draw was honest, even if the preventive security protocols were circumvented and no visible traces of fraud were left. Draw fraud detection is built into the draw system, as it is a design factor of the original RNG method.

[1] Szrek2Solutions designed and patented auditable RNG method, implemented the RNG platform for draw games (lotto, numbers, keno, bingo, raffle, 2nd chance and instant games; provided Trusted Draw™, Trusted Play™ and Trusted Audit™ systems to lotteries and game operators since 2005, including Danish Lottery, Lottomatica Italy, Sisal Italy, Luxemburg Lottery, South Carolina Lottery, Georgia Lottery, Oregon Lottery, Texas Lottery.

The auditable RNG method relies on properties of digital signatures[2]. For winning numbers generation and verification digital signatures of draw data are used as RNG seeds. Thanks to digital signature properties, since winning numbers are derived from digital signatures, they can be also verified.

A special 'audit' file is created by Trusted Draw™ system during the draw. The audit file includes critical draw data in digitally signed format and verification of this data detects if there was any fraud attempt; this can be carried out immediately after the draw or at a later time, when necessary. This audit file itself cannot be manipulated as any manipulation of digital signatures will be detected.

To prove draw integrity, the audit file created during the draw time is verified and detects:

1. Manipulation of winning numbers drawn
2. Manipulation of draw time
3. Every RNG use.

Trusted Draw, being an auditable RNG with fraud detection, works also as a deterrent, since a fraud attempt will be always discovered and dealt with.

Fraud Detection RNG Requirement

The industry introduced many security technologies to protect its integrity: ICS (internal control systems) are used by most lotteries to verify on-line systems. Some European and Israeli lotteries use digital time stamping to safeguard bets. GGuard and similar technologies are used to protect security of lottery tickets. RNG audit and fraud detection technology has not been usually required, even though draws are critical elements of the lottery and RNGs are a big public opinion item. Lotteries need to introduce requirements for auditable and provably secure RNG draws with fraud detection. As we have seen physical security measures and reliance on human honesty are not always sufficient to enforce draw integrity. This serious risk exposure is present for many RNG based drawing machines: standalone or off-line and drawing machines connected to on-line systems (such as Bingo and Keno). These potential integrity issues should also be addressed for instant win games on the internet that are entering the US market.

Conclusion – Call to Action

We presented a potentially serious breach of lottery integrity. One case is being investigated, at this time we do not know if there are more. Even a single case carries a potential serious liability to the industry - higher than the cost of all the RNG drawing machines for all Lotteries combined. The industry

[2] A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Digital signatures provide admitted evidence in the court of law. Signatures are created using a secret private key and verified by a known public key. In addition digital signatures have random properties. Combination of these properties in Szrek2Solutions patented method allows random numbers generation and verification. To ensure security of private key and digital signing process, NIST certified tamper proof hardware security module (HSM) is used by Trusted Draw to generate digital signatures and random numbers.

needs to recognize the risks of exposure to RNG draw fraud and eliminate it. In order to protect the lottery industry, computerized drawing machines need to provide technology comparable to Trusted Draw. It is imperative that the industry leaders set a new requirement standard for auditable RNG and demand secure RNG solutions, such that any manipulation of winning numbers or draw time can be determined at any time, regardless of the followed security protocols.

Szrek2Solutions will be glad to further explain the technology and assist in deployment of its secure Trusted Draw system.

References:

(1) "CHARGES FILED IN HOT LOTTO® JACKPOT INVESTIGATION, LOTTERY ISSUES STATEMENT" http://www.dps.state.ia.us/commis/pib/Releases/2015/IALotteryStatement_HotLotto-ChargesFiled.pdf

(2) Iowa TV station news program and news article http://www.kcci.com/news/lottery-security-director-fired-after-charges-filed-in-hot-lotto-case/30763858.

(3) "Method of generating unpredictable and auditable random numbers". US patent 6,934,846

(4) "Trusted Draw™ - Secure Computerized Drawing System", http://www.szrek.com/Trusted_Draw_white_paper.pdf

(5) "Electronic Draw Security Recommendations", http://www.szrek.com/electronic_draw_recommendations.pdf

(6) Various whitepapers about Szrek2Solutions auditable technology and RNG products : http://www.szrek2solutions.com/s2s_products.html

(7) Wikipedia entry on digital signature http://en.wikipedia.org/wiki/Digital_signature