Trusted Draw Security

Publicized fraud cases[i] of RNG drawing systems have negative impact on all lotteries, no matter where they occurred, so it is in the interest of all lotteries to deploy secure RNG solutions with fraud detection.

S2S developed and patented such RNG solution, which provides a conclusive proof of draw integrity, even if the draw system was compromised and no traces of fraud were left. Trusted Draw™ system creates a proof of draw integrity, which cannot be manipulated and can be independently verified.

RNG Security Concerns

Traditional RNG Solutions

There are inherent problems with traditional RNG systems which are based solely on preventive security measures and security procedures. With sufficient skills, knowledge and access to system security these measures and procedures can be broken. In addition visible traces of such break-in can be removed. So while many preventive security practices are good, they are not sufficient, as all ways of attacking the system are not known and may not be predicted.

Once the RNG system is taken over by an attacker, the system cannot be trusted. Here are some examples why:

1. There is a procedure used to verify hashes (checksums) of the draw system programs created at the time of certification. If the values match, draw manager and auditor are confident that the programs used to generate random numbers are the ones that were certified, so they are correct. However, they can be fooled: the generation program is started by clicking on the RNG program icon or key. The icon/key may actually point to another, substituted fraudulent program. This fact will not be verified. While we can add additional verification steps to the security checklist, there are many more examples of vulnerabilities, which cannot all be predicted and protected against.
2. Vectors of future attacks are unknown as is vulnerability of the deployed solutions, for example:
    - Off-line RNG systems do not go through (regular) OS (operating system) updates. During the time of deployment some vulnerabilities of the OSs are discovered and could be used to take over the RNG OS.
    - Inside RNG system knowledge may not even be needed for a successful attack. If an attacker was able to back up the RNG system, the system can be recreated to prepare for the attack. In fact the backup does not have to be of the specific system. If a vendor provides the same solution in many places, a copy of the programs of any one of them may be sufficient to stage a fraudulent draw.
3. Rogue tools installed on the RNG system will go most likely undetected. This is because there are many different programs residing on the system. While it is simple to verify details of some specific programs, it is very difficult to verify everything that is on the system. Plus these rogue tools can be removed after the attack.

It is important to realize that vulnerability detection might be out of control of the lottery. The RNG systems with only preventive security measures and procedures do not provide protection in case of an attack by a skilled insider or collusion of insiders.

S2S Draw Systems Security and Fraud Detection

S2S created RNG solution addressing limitations of traditional RNG draw technology. In addition to preventive security measures S2S Trusted Draw offers fraud detection technology. Fraud detection technology is provided as an independent Trusted Audit™ system or audit service.

1. Following are highlights of S2S RNG solutions used for draw fraud prevention and detection.
   Preventive methods:
   i. Tamper resistant environment. All files: executables, configurations, data, logs, reports, etc. are under system protection and no user, even RNG system admin, has privileges to write/modify/delete any files. Critical data structures such as product configurations cannot be modified by user/client and are protected by secure hashes (HMAC).
   ii. Two+ logins. Drawing requires draw manager and draw auditor to log in.
   iii. Time window. Drawing can be configured to be executed only in a defined time window.
   iv. Real time monitoring of key resources such as integrity of files, correctness of RNG seed.
   v. Extensive logging and log review facility. Activity log and console log with viewing tools.
   Fraud detection methods:
   i. Analysis of internal RNG logs and reports. As long as RNG system was not compromised analysis of RNG internal logs allows detection of an attack. Unless an attack was skilled, there will be traces of an attack if the system was compromised.
   ii. An independent Audit system or service is optionally provided to ultimately prove RNG integrity. Audit system provides a conclusive verification of the RNG system integrity.
2. S2S's RNG methodology offers proof if draw numbers were manipulated, if draw time was changed, and accounts for each use of RNG - this prevents 'phishing' for the desired winning numbers.
3. To obtain a proof of draw integrity a single file is exported from the RNG system for verification. It can be verified immediately, or any time later as long as the file is stored. In the Iowa case S2S system would be able to definitively prove if there was a draw fraud involved.
4. **While it may seem contradictory, the proof of integrity does not require integrity of the RNG system itself. Even if the S2S's Trusted Draw was compromised by skilled attackers who manipulated data, programs, hardware, and removed traces of attack, they would still not be able to fix a draw without detection. Even in a case of collusion of draw manager, draw auditor and use of the rogue software, the drawing could not be conducted fraudulently without detection.**
5. Summary of technology behind S2S RNG method:
   i. Every random number is a function of RNG seed, such that Random Number = f (RNG Seed). Once we can prove integrity of the RNG seed, we can also prove integrity of random numbers derived from it. The essence of S2S technology is securing RNG seed in a way that it cannot be manipulated without detection.

ii. Digital signature is a schema that allows verifying integrity of data. There is a private key for signing the data, and a public key for verifying the data. Signature is an unpredictable, "random" string of bits that can be verified by the public key.

iii. To generate random numbers S2S uses digital signatures as RNG seeds. This is different from digitally signing draw data AFTER the draw. Signing already generated data or time only proves that they were not changed later. However they might have been already compromised.

iv. Digital signatures are performed by Hardware Security Module (HSM). These HSMs are NIST certified tamper evident crypto devices with embedded Real Time Clock (RTC) and a signature counter (sequencer). The private (signing key) is protected by HSM and is never disclosed outside of HSM. Only a public key is provided outside for verification. During the signing process RTC and the sequencer are signed, sequencer is also incremented. This accomplishes a few key points: provides a proof of generation time (signed HSM internal clock and RNG system clock), every RNG is accounted for (sequencer value) and data signed is different each time, so the seeds will never repeat. As a result there is a signature/RNG seed from which every random number is created and can be verified. These signatures together with some additional data are written to the signature log file.

v. The signature log file is used by an independent Trusted Audit system to verify draw integrity. Audit system authenticates digital signatures/RNG seeds and recreates from them generated random numbers. It creates reports that contain all critical draw information which are then verified to prove integrity. Audit system can be used for draw verification immediately after the draw or later, as long as signature log file is preserved. Audit system functions are backward compatible and game independent, so changes on draw system will not impact ability to audit. If a draw fraud is suspected, it is enough to perform draw verification on the Audit system. There is no need to verify the draw system, which may have been compromised and unable to prove draw fraud.

Conclusion

Traditional RNG systems are vulnerable to hard to detect insider attacks. To protect their RNG integrity lotteries should use fraud detection technology. The RNG solution, as provided by S2S, enhances traditional RNG security by providing irrefutable fraud detection. The proposed solution is similar to current lottery solutions, where on-line lottery systems are verified by the independent ICS systems. S2S's Trusted Audit system mathematically proves integrity of the generated draw numbers, it proves the time of the generation and accounts for every generated random number. Audit/verification can be performed any time: immediately after a draw or any time later, even years later. As a full proof detection of fraud, S2S technology works also as a fraud deterrent - once fraud is always detected, there is no reason to commit it. Trusted Audit system is offered as an independent system or as an audit service.

This article describes a fraud case that is being investigated in 2015 in Iowa http://www.desmoinesregister.com/story/news/crime-and-courts/2015/04/13/hot-lotto-ticket-trial-delayed/25715155/http://www.iprt.iastate.