

Electronic Draw Security Recommendations

Background

Traditional computerized drawing machines rely solely on preventive security. Procedural measures are employed to minimize the risk of fraud. In practice, skilled insiders with access to the machines may circumvent preventive security system without being detected.¹ Random number generation method is certified to produce random numbers but there is no audit trail proving integrity of the random number generation process. Existing audit trail doesn't include random numbers generation process, hence it is non-conclusive - one cannot guarantee that there was no fraud in random numbers generation. In many implementations the audit trail is very limited, and it can be altered – it is not tamper proof (or tamper evident). Consequently it does not guarantee that data, time or process was not manipulated.

The case of security of traditional mechanical drawing machines is different – they are hard to defraud providing proper preventive security and audit procedures are in place. Traditional draw machines use relatively simple mechanical devices for draw process; they do not rely on computer software, firmware and algorithms that are susceptible to fraud. They have no passwords that a hacker or insider may break to defraud the system, no secret data or hidden features that could be exposed, software that could be disassembled, algorithms that could be misused. There is no danger of code temporarily replaced and restored back after defrauding the system; mechanical draw results cannot be obtained earlier on the device and demonstrated later.

There are many different security aspects of computerized drawing machines, which may be tampered with internally, that are not visible from outside and which cannot be conclusively measured or accounted for. To address the weaknesses of computerized drawings Szrek2Solutions developed a patent pending RUN+A (Random Unpredictable Numbers with Audit) methodology, allowing detection of fraud in generation of random numbers. RUN+A solution, using modern cryptographic techniques, guarantees that random numbers themselves can be audited and verified after their creation, even years later. Not only random numbers can be verified but also the time when generation took place and generation hardware can be verified. Strength of RUN+A approach is that it uses only publicly approved and scrutinized standard cryptographic algorithms in random numbers generation. The algorithms used in RUN+A were analyzed and certified to be both unpredictable and random (lack of patterns). In RUN+A method there is no secret data that could be exposed; access to software, passwords and hardware does not give an insider any advantage in manipulating or predicting draw results. Draw numbers generated using RUN+A have cryptographic strength of 1024 bit RSA signatures.

Recommendations

Most major lottery processes are audited to prove their integrity; except for electronic draw results generation and assignment of instant win bets, which are key lottery processes but are not 'provably auditable'. By 'provably auditable' we mean a use of conclusive procedure that uncovers any fraud attempts. It complements preventive security measures and goes beyond them,

¹ NY Times, February 28, 2004, John Schwartz—"Electronic Vote Faces Big Test Of Its Security": conspiracy among slot machine workers who rigged the devices with software patches that shifted the odds when a particular sequence of coins was entered. The fraud went undetected from 1992 until 1996, after the ringleader, Ronald Harris, won a \$100,000 jackpot with an accomplice in Atlantic City. Mr. Harris, a gaming regulator at the time, was convicted of racketeering."

detecting any fraud attempts assuming security has been compromised. Only if the fraud is always successfully detected, the fraud is not going to happen².

We believe that such key lottery processes as electronic draw results generation should be provably auditable. Computerized drawing machines create multi-million dollars payouts and temptation may be high to defraud them. Given the spread of electronic drawing machines the attempts to defraud them have likely already taken place. A Harris case in Atlantic City has been detected (by chance) and publicized³, but there may have been more cases that we don't know about, as they are very hard to detect w/o ability to audit.

Following is a list of proposed requirements for computerized drawing machines:

- General Drawing machine requirements:
 - Numbers generated cannot be predictable and need to have required distribution.
 - Only standard, publicly scrutinized algorithms should be used for Random Numbers Generation.
 - Neither private algorithms nor non-auditable physical processes should be used, as these can have hidden weaknesses or features.
 - Every drawing system should consist of both an electronic drawing machine and audit/verification system.
 - Audit/verification system needs to certify: numbers drawn, draw time, drawing machine.
 - Capability to easily analyze actual draw results for statistical properties should be present. RNG statistical analyses, as well as any RNG certification (such as by GLI or other organization) does not prove that the drawing machine is or is going to be secure; it certifies that the results have random properties, and can not be predicted.
- Preventive security ("perimeter/access protection"):
 - Access to the drawing computer (PC) should be limited to the computer operation, administrative, and drawing personnel. The access should be only allowed during their "normal" activity time.
 - "Standard" securing of PC should be put in place (activity log, strong passwords, limited privileges accounts, no guest accounts, up to date system patches, antivirus protection, internal firewall, encryption, etc)
 - Physical security using special enclosures and locks.
 - Biometrical recognition or a hardware token secured access is recommended as a complementary means of authentication to password authentication.
 - LAN access security.
 - Additional security measures applied in the jurisdiction.
- Provable audit ability - protection against sophisticated attacks requires ability of provable audit after the drawing. In this case it is assumed that the attacker can gain illegally or legally (an insider) access to Drawing PC and/or its workings:
 - Numbers drawn should be auditable themselves. Audit needs to prove that those specific numbers were the results of the specific random number generation, not

² Bruce Schneier <http://www.schneier.com/essay-028.html> : **Attack Prevention vs. Attack Detection**

Most cryptographic systems rely on prevention as their sole means of defense... Defense should never be that narrow. A strong system also tries to detect abuse and to contain the effects of any attack. One of our fundamental design principles is that sooner or later, every system will be successfully attacked, probably in a completely unexpected way and with unexpected consequences... Systems have to do more than detect an attack: they must also be able to produce evidence that can convince a judge and jury of guilt.

³ Article about Harris: <http://www.americancasinoguide.com/Tips/slot-cheat.shtml>

merely to prove that these numbers were presented as numbers drawn during the generation process.

- Drawing audit needs to prove the time of the random numbers generation. Generation time is not necessarily the same time as the drawing machine time. Attacker could manipulate the computer time. In other words, the machine should provide an independent clock that cannot be manipulated internally or externally.
- Access to the physical computer, software, algorithms, secret data stored in the computer and passwords should not be sufficient to learn what numbers could be generated or to be able to circumvent the generation process undetected. In other words, even if all the above information was available, in no way should this affect drawing process and its audit ability
- Any “critical secret data” used for generation (such as seeds, secret keys, etc.) should be stored and controlled in a certified tamper evident or tamper proof method. An example of such certification is FIPS140-1 level 2 or FIPS140-1 level 3
- There should be no password allowing “unlocking” of critical secret data or method for reading critical secret data from the machine.
- Audit/verification system needs to have a full-proof mechanism to account for all random number generator uses, to avoid certain type of attacks
- Tampering with audit information should be detectable
- One should be able to run audit process any time after the draw, even years after. Audit data needs to be kept for periods according to local jurisdiction requirements.