

Security Requirements for Electronic Drawing

Electronic drawing machines use random number generators (RNG) for generation of winning data. It is essential that the RNG used is verified to supply statistically well distributed numbers. Most computerized draw machine suppliers focus on the RNG, and claim security of the draw solely based on goodness of the RNG. However this is not a sufficient requirement for an electronic drawing system. Since drawing is “a heart and soul” of every game of chance with a draw, security of the overall winning numbers generation process need to be addressed, including the RNG and all software and hardware used in the generation and delivery of winning game results.

Below we have formulated most critical requirements for the security of electronic draw process:

1. The generated draw **outcomes**, actual wining numbers, have to be **provably secure**.
2. The **process** of generation of draw outcomes has to be also provably **secure**.
3. Each draw outcome generation has to be **accounted for**.
4. **Verification functionality** for draw outcomes should exist and be easy to use.
5. Generated draw outcomes have to meet **desired statistical properties**.
6. Draw outcomes can **not** be **predictable**.
7. There should be **no proprietary hardware or algorithms** used to ensure security.
8. Any hardware protecting critical information should be **tamper evident or tamper proof**.
9. System must be **resilient against attacks**.
10. There should be **no single point of failure**.

1. Provably Secure Outcomes

It is important in an electronic drawing system to ensure that for every individual draw outcome generated it can be verified that it was the actual outcome generated by the system. It is not sufficient to prove that generated numbers have good statistical properties. It should be possible to prove that generated numbers were not altered in any way in the process of draw generation, e.g. generated by an insider ahead of time in purpose to defraud the system.

2. Provably Secure Process

One of the basic elements of the security of an electronic draw is safeguarding the whole process, not only the generation of draw outcomes. One needs to prove that draw outcomes were generated at the right designated time, on the proper machine, in right sequence, etc, not for example ahead of time, so the attacker could use these numbers to buy winning transactions. Adherence to physical security requirements, data privacy, users authentication, data integrity are other important factors required to ensure secure process of electronic draw.

3. Accountability of Draw Outcomes

One of possible attacks against an electronic drawing system is that an attacker may try to use the system to generate many different draw outcomes ahead of time and pick only ‘suitable’ ones. This way of attack is called *fishing*. To prevent those attacks every draw outcome generation in the draw system should be accounted for.

4. Verification Functionality

Verification of the draw process and draw numbers, any time after the draw, is needed to offer assurance of integrity. Verification capability should not be limited in time, as some system abuses may not be identified at the early stage. There should be sufficient information provided about the draw process to allow an audit by a 3-rd party.

5. Desired Statistical Properties

Electronic draw has to ensure that draw outcomes have desired statistical properties according to specific game requirements, otherwise clever players or dishonest insiders may take advantage of a bias of numbers drawn.

1. Generated draw outcomes have to have desired statistical properties.

2. RNG has to ensure unbiased generation of random numbers – strictly no bias can be present.¹
3. RNG can generate random numbers in various formats: it can be a big integer number, double float number or even a good generator for 0/1 bit outcome that could be repeated many times.

6. Draw Outcomes not Predictable

Electronic draw system has to guarantee that draw outcomes can not be in any way predictable.

1. There must be no internal data, at any internal state of the draw system, that could be exposed to predict the draw outcomes.
2. Knowledge of any algorithm used by the draw system should not give any advantage in predicting draw outcomes.
3. Random number generation should not be repeatable, so the attacker cannot have an advantage of generating the same outcomes ahead of time.
4. The same or different hardware should not allow recreating of the draw outcomes.

7. No Proprietary Hardware or Algorithms

Proprietary algorithm or hardware can never go through sufficient peer review and tests – there is always a significant risk of a defect, so they should not be regarded as secure. Generally there is a long process ensuring that any new algorithm is assumed secure, during which the algorithm is made public. The algorithm will go through very thorough independent evaluation by the specialists. Good examples of algorithms that went through such review are encryption algorithms, digital signature algorithms, and cryptographic hash algorithms. Any algorithm whose strength relies on its secrecy should be regarded as insecure. *There is no security by obscurity.*

8. Tamper Evident or Tamper Proof Hardware

Any 'secret' information used in the draw numbers generation should never be available outside of the secure hardware. E.g. private encryption key stored in a secure cryptographic hardware can not be exposed. Such secure hardware should be certified to be either tamper evident or tamper proof. For example, FIPS 140-1 Level 2 or 3 Certification provides such assurance.

9. Resilience against Attacks

Following types of attacks are especially critical for the electronic draw system:

1. Time related attacks (e.g. clock corruption)
2. Random numbers/draw outcomes exchange or modification
3. RNG bias or game matrix change
4. Fishing and replay attacks
5. Masquerading (e.g.: man-in-the-middle, ignoring the results, exchange of the program, exchange of the hardware, connection hijacking)

Electronic draw system has to be resilient against any attacks, including the most serious insider attacks. This means that any fraud attempt would either be resisted by the system, or if it can not be resisted, it will be detectable. Electronic draw system should either resist an attack or detect that attack took place. If there was any attack on draw outcome generation the nature of the problem should be auditable.

10. No Single Point of Failure

There can not be any single point of failure in the electronic draw system operation. This refers to software, hardware and data and is needed to guarantee smooth operation of the draw system and general availability of the draw system outputs, independent of hardware and software defects or loss of data.

¹ This is a non-trivial issue. E.g. if one generates a real number $[0,1)$ and absolutely no bias is allowed, for generation of the number 1, 2 or 3, it is not enough to divide the interval $[0,1)$ into 3 equal parts and choose the value based on the random interval. One of the 3 outcomes will have an extremely small chance to be more likely. This is OK for almost all applications, however not when no bias is allowed.