

Electronic Drawing Machines – Security Threats

Electronic drawing machines are exposed to many security threats. Even if the machine is supervised in a locked room, protected by a special enclosure and camera, connected using a private network and a custom protocol, the environment may be insecure.

Following is a sample list of possible security threats:

1. **Physical connection may be 'hijacked'** – attacker, insider or in some environments also an outsider, may remove a physical connection from the authorized drawing machine and connect it to another device. This kind of attack is relatively easy in any communication environment. This could also be accomplished by manipulating network routers and switches.
2. **Logical connection may be 'hijacked'** – attacker may masquerade on the protocol level as an authorized machine. This kind of attack is especially easy in the TCP/IP world. It is also a problem for other environments.
3. **Drawing program may be exchanged** locally, when the system is not supervised, or exchanged remotely. After it is restored there may be no proof of change left. This may be handled by a script 'hidden' in the drawing machine. This script may destroy itself when finished.
4. **Drawing program may have hidden features** allowing attacker generation of specific numbers.
5. **Drawing algorithm may be programmed with a 'desired' bias**, causing some results/combinations to happen more often. Such a bias may not always be detectable by the statistical analysis.
6. **Drawing algorithm may be predictable** to enable the attacker to predetermine the results – for example a finite number of states that the machine goes through during its operation may allow attacker to predetermine the draw numbers.
7. **Drawing algorithm may be crypto insecure**. Quite often pseudo random numbers generators are used for drawings. These algorithms are breakable.
8. **Algorithms may rely on secrecy** of proprietary algorithms, secrecy of data or other elements that are not verifiable. Each one of these elements may become exposed and drawing process may be compromised.
9. **Time related attacks:**
 - a. Draws may be shifted in 'phase', so that the actual results for draw data are generated earlier.
 - b. Client software (host machine running the game) may be manipulated to request draw results earlier.
 - c. Clock may be 'corrupted' and the results could be available earlier.
 - d. Etc
10. **Man-in-the-middle attack:** attacker can position him/herself in the middle between a client and a drawing machine to gain control over the process of 'delivery' of draw numbers. This may be accomplished by loading a filtering program onto the client machine or inserting a filter device on the network.
11. **Ignoring of drawing machine results**. Gaming software may be manipulated to produce its own draw numbers and simply ignore drawing machine results.

The above list is not complete! It only provides examples of security issues that should be considered for electronic draw machines. Main source of exposure comes from the dependence on physical security and integrity and software security and integrity. This is very hard to enforce: there are many vulnerable points for attack (connections, cables, routers, drawing machine, host machine software, drawing machine software, drawing machine data, corruption of the clock...).

A sophisticated attack is very hard to trace or detect, as there is no capability to audit neither the numbers drawn nor actual event time. Legacy electronic drawing machines rely on statistical analysis to check integrity of drawn numbers. **Statistical analysis does not prove draw integrity**; it only shows that the drawn numbers look random.

Trusted Draw™ and Trusted Play™ technology is addressing these exposure areas. It offers ultimate security of a drawing process and its verification:

1. **Tamper proof¹ or tamper evident² security** for draw number generation.
2. **Use of Unpredictable Auditable Random Numbers method³** for the generation of random numbers. Random numbers generated cannot be predicted, yet they can be verified in a fully conclusive manner - that these are the only numbers that could have been generated.

3. **Capability to audit drawn numbers** themselves to verify that these are the correct numbers.
4. **Tamper evident audit trail** of drawn numbers generation.
5. **Audit trail logged to multiple media** to avoid single point of failure.
6. **Tamper evident trail for the actual time** when draw was generated.
7. **Audit trail for every attempt** to generate draw data.
8. **Authentication** each time data is exchanged.
9. **No proprietary algorithms or secret elements** that could be exposed.
10. **Security industry proven and scrutinized methods** to generate and audit any information.
11. **Certified and field proven cryptographic hardware** used; FIPS 140-2 and FIPS 140-3 certified.
12. **Providing a simple audit process** for draw results.

Trusted Draw™ ensures integrity of the draw process by using modern cryptographic hardware and digital signatures technology. This technology has developed over the last 25 years and with the growth of Internet became a security commodity. It is currently widely used for authentication in commerce and governmental agencies.

Following are some additional highlights of Trusted Draw™ and Trusted Play™ products:

1. **Trusted Draw™ ensures good statistical properties** of draw data by using cryptographic algorithms that were already proven for its good statistical properties. Any bias is eliminated during the generation of random numbers.
2. **Data generated with Trusted Draw™ went through very thorough statistical analysis** using Diehard Battery of Tests of Randomness⁴.
3. **Trusted Draw™ has a built-in statistical analysis** of generated data. Tests are done for frequency of individual numbers and for frequency of numbers' combinations.
4. **Trusted Draw™ supports generating of large files of random data**, so randomness of data can be verified by an independent organization.
5. The design of Trusted Draw™ solution was **analyzed and approved by a known expert in the field of data security**⁵.

¹ Tamper proof relates to devices that self destroy at a tampering attempt

² Tamper evident describes devices that capture or otherwise detect a tampering attempt

³ Szrek2Solutions has a pending patent for the Unpredictable Auditable Random Numbers method

⁴ George Marsaglia Randomness Test Suite - <http://www.csis.hku.hk/~diehard/>

⁵ The design of the Trusted Draw™ and Trusted Play™ was analyzed and approved by Russ Housley, one of the leading world experts in the field of PKI (Public Key Infrastructure), (<http://www.vigilsec.com>). Russ's report on trusted products technology is available upon request.