

Does Security Matter?

Security and integrity of a draw are critical elements of lottery games.

Any publicized case of defrauding of a draw could have a disastrous effect on the whole industry as they currently all have a very limited audit capability.

Over the years the industry has seen many instances of manipulation of mechanical drawing machines. Electronic drawing systems are also exposed to many security threats. High availability of computer technology combined with lack of audit ability of the results make them an easy target for fraud.

Especially dangerous are the insider attacks, because they are the hardest to detect.



Security Threats

to electronic drawing systems include:

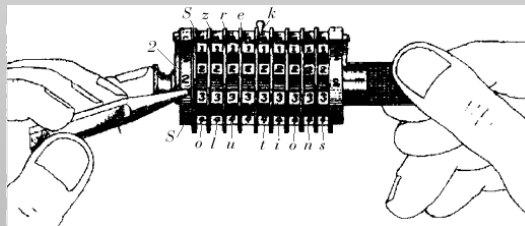
- φ Outcome generation **program may be exchanged or overwritten**, locally or remotely.
- φ **Program may have hidden features** allowing attacker generation of specific numbers.
- φ **May be programmed with a bias** causing some combinations to happen more often, undetectably by statistical analysis.
- φ **May be predictable** to allow the attacker to predetermine the outcomes.
- φ **Algorithms may rely on secrecy** of data or other elements that are not verifiable; these elements may become exposed and the generation process may be compromised.
- φ **Time-related attacks**: drawing time shifted to produce results earlier, Clock 'corrupted' to make results available earlier.
- φ **Corrupted personnel** conducting a draw.

Szrek2Solutions

is an international company dedicated to providing innovative secure solutions for the gaming industry. Our products, Trusted Play™ and Trusted Draw™, offer the best random number security needed in today's insecure world.

We provide end-to-end product implementation. Our services include customization, integration, product support and consulting. We have 50 years of experience in lottery industry in system design and implementation. Our area of expertise includes:

- Game design
- System and data security
- System architecture and design
- Products integration
- Technical evaluation
- Communication consulting
- Requirements gathering



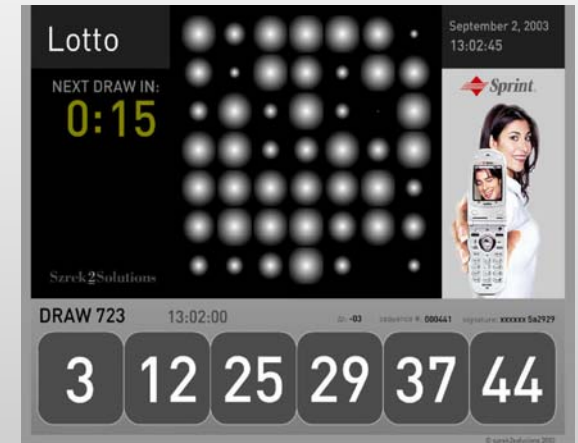
Szrek2Solutions

60 Spencer Avenue
East Greenwich, RI 02818, USA
Phone/Fax: 401-398-0395
Email: info@szrek.com
Website: www.szrek.com

Copyright © 2003 Szrek2Solutions

Szrek2Solutions

Trusted Draw™ Secure Electronic Drawing System



When I play I trust

www.szrek.com



Trusted Draw™

Solution to Market Needs

Trusted Draw™ is an innovative secure computerized drawing system for games of chance, with built-in integrity verification. Trusted Draw verification will detect any potential fraud, including insider attacks.

Fact For the last few years lotteries have been introducing computerized drawing machines to reduce cost and provide more game excitement (e.g. games with frequent draws).

Problem Currently used computerized drawing machines are not sufficiently secure and are vulnerable to insider attacks.

Solution Trusted Draw™ is a tamper proof computerized drawing system designed to address the market needs:

- ⇒ It uses modern cryptographic hardware and software.
- ⇒ Numbers drawn are unpredictable and have desired statistical properties.
- ⇒ Audit verifies draw time and unequivocally verifies numbers drawn.
- ⇒ Audit certifies that there was no fraud during the draw process.
- ⇒ It is specifically designed to detect insider attacks; even years after the draws are held.
- ⇒ It is based on a patent-pending method of generating Random Unpredictable Numbers w/Audit (RUN-A) and securing electronic draw.
- ⇒ It is flexible and easy to use.
- ⇒ It is priced competitively.
- ⇒ Single system handles draws for many games, further reducing cost.
- ⇒ Most games of chance are supported.

Trusted Draw Components

φ Trusted Draw Engine

- Tamper evident draw numbers generation
- Time stamp
- Audit data logging
- Robust and reliable



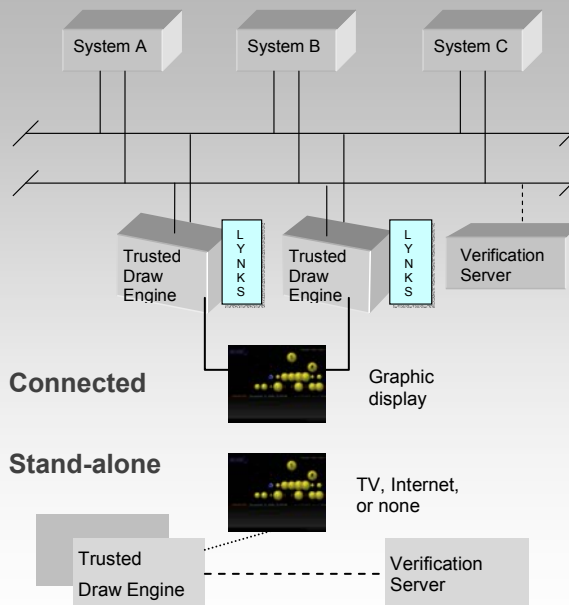
φ Cryptographic Card

- Digital signing
- Tamper evident device, FIPS 140-1 Level 2 Compliant
- High-assurance security mechanisms
- Enhanced firmware for gaming security
- Incorruptible Real Time Clock
- Protects all secret Information

φ Verification System

- Stand alone or integrated with ICS
- Verification of draw numbers and draw time
- Detection of “missing” or “extra” draws
- Generates detailed draws audit report
- Runs basic statistical tests

φ Trusted Draw Application



φ Trusted Draw Application (continued)

- Connected to the on-line gaming system or stand-alone
 - Flexible and simple user interface
 - Support for all games of chance
 - Many games already in the game library: keno, bingo, lotto, numbers, joker/kicker, passive games, multi-matrix games, e.g. PowerBall
- ### φ Bubble© Graphics Display
- TV & Internet ready
 - Copyrighted graphics design
 - Parameterized application
 - Simple secure file interface
 - Promotional space
 - Graphic library of games includes keno numbers and lotto (single and multi-matrix)

