

NASPL Security Directors Meeting December 4, 2003

- ◆ About Us
- ◆ Problem Definition
- ◆ Threats Against Electronic Drawing Machines
- ◆ Trusted Draw™ Solution
- ◆ Technology Used
- ◆ Product Components
- ◆ Trusted Play™
- ◆ Product Demo
- ◆ Q&A



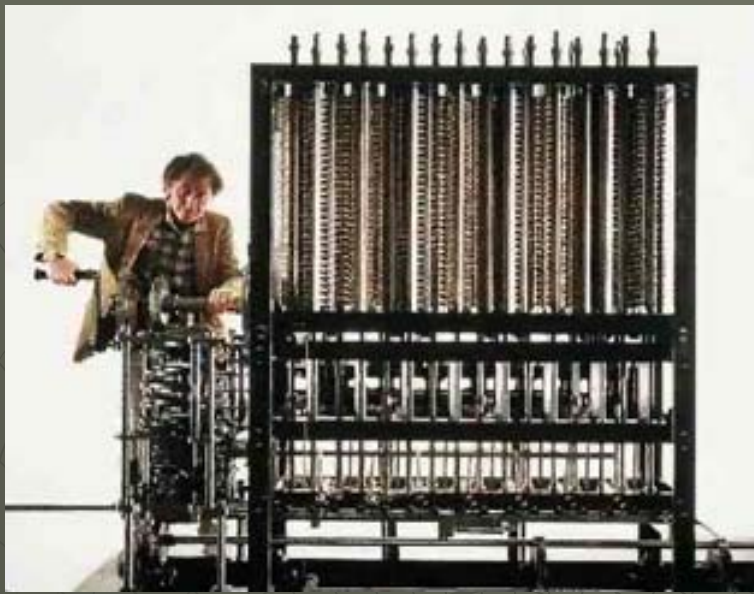


Szrek2Solutions



About Us

- ◆ Szrek2Solutions LLC started in 2003
 - Founders each have 20+ years experience at GTECH
 - ◆ Walter-system architect, senior technical consultant
 - ◆ Irena-software director, project & product manager
- ◆ International gaming product and service company
 - Secure software systems solutions
 - Data security & system integrity
 - Product development and software consulting
- ◆ Szrek2Solutions Accomplishments
 - Invented 'Unpredictable Auditable Random Numbers' method—patent pending
 - Introduced Trusted Draw™ tamper evident electronic draw system at NASPL 2003
- ◆ Our coordinates:
60 Spencer Ave, East Greenwich, RI 02818, USA
www.szrek.com e-mail: irena@szrek.com tel. 1-401-398-0395



Problem Definition

- ◆ Today 30% of lotteries use electronic drawing machines
- ◆ This trend will grow, as they are cheaper, easier to operate, offer new values – e.g. entertainment
- ◆ Security of existing computerized drawing machines is not satisfactory for today's 'connected' & computer savvy world:
 - Statistical analysis of draw results – does not prove system security
 - Physical security of draw machine – can be circumvented
 - Dependence on personnel integrity – 80% of computer fraud by insiders
 - Insider can manipulate the draw outcome w/o detection
- ◆ High level of security and ability to audit is key for all Lottery processes
- ◆ Current electronic drawing machines do not offer ability to audit draw numbers, draw time or generation process

Security Threats

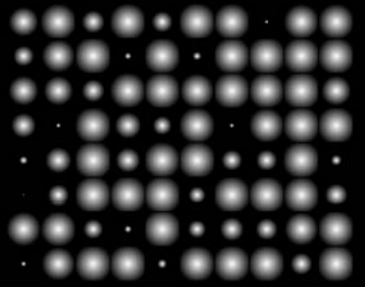



- ◆ Time related attacks
 - Clock corruption
 - Earlier drawing
- ◆ Drawn numbers bias
- ◆ Masquerading:
 - ignoring the results
 - exchange of the program
 - exchange of the hardware
 - connection hijacking
 - man-in-the-middle
- ◆ Fishing and replay attacks

REANO May 31, 2003
20:25:39

Szrek2Solutions

NEXT DRAW IN:
0:12

DRAW 107 20:24:50 Δ 4534 sequence # 3363 signature: xxxxxx 997241

6	12	21	23	24	25	30	34	37	45
47	49	51	57	58	64	66	69	71	73

© szrek2solutions 2003

Szrek2Solutions

Solution:

Trusted Draw™

Innovative Secure Electronic Drawing System with State-of-the-art Graphics

- ◆ Random and fair auditable draw results for any game of chance: lotto, keno, bingo, numbers , multi-matrix, cards, dice, ...
- ◆ Designed to provide ultimate draw security and to protect against skilled insider attack – detects any attack
- ◆ No other product offers draw security nearly as strong
- ◆ Use of Unpredictable Auditable Random Numbers patent-pending method proves the integrity of the system:
 - Audit of the draw process (drawn numbers, draw time, more)
 - No secret element can be exposed by insider or auditor (data or algorithm)
 - Use of tamper evident cryptographic hardware, digital signatures and time stamping
 - Only standard and proven cryptographic methods used

Technology Used

Asymmetric (Public) Key Cryptography

- ◆ Digital signatures are source for draw numbers
- ◆ Digital signatures use two keys:
 - **private** to sign and **public** to verify
- ◆ Tamper evident crypto processor protects private key and provides real time clock
- ◆ Became commodity in last 10 years
- ◆ Used in banking and financial services
 - securing transactions
 - securing communication
- ◆ Used in high security governmental applications

Szrek2Solutions uses this technology for 2 products:

- ◆ Trusted Draw™ enables secure drawing
- ◆ Trusted Play™ enables secure “instant” betting



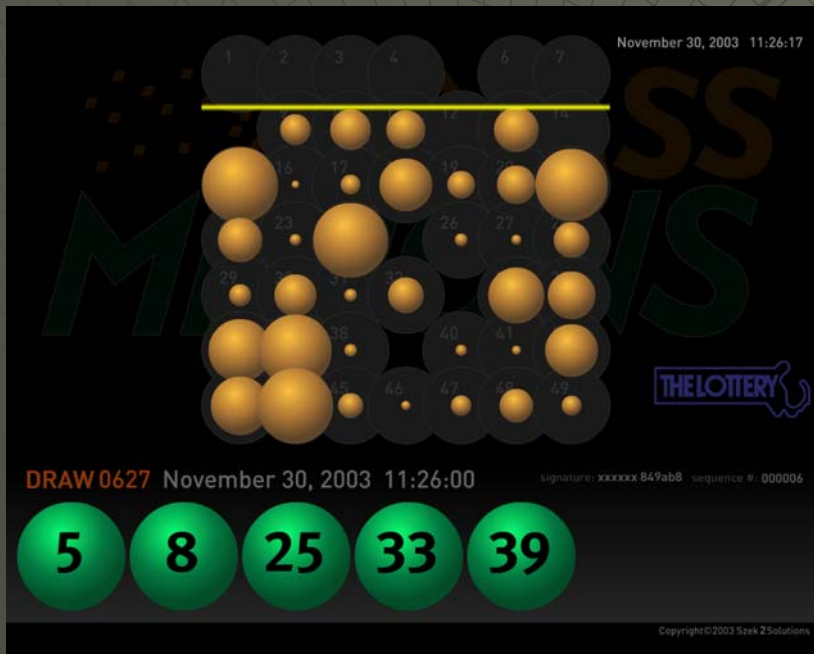
Trusted Draw™ Components

- ◆ Trusted Draw™ Drawing Application
 - Stand alone drawing machine or
 - Connected to the on-line gaming system
 - With or without graphics
- ◆ Trusted Draw™ Engine
 - Tamper Evident Draw Numbers Generation
 - Time Stamp
 - Audit Data Logging
 - Robust and Reliable
- ◆ LYNKS Privacy Card for 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



Trusted Draw™ Components continued

- ◆ Trusted Draw Audit 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



- ◆ Bubble© Graphics display
 - TV & Internet Ready
 - Copyrighted Graphics Design
 - Parameterized Application
 - Simple Secure file interface
 - Promotional space

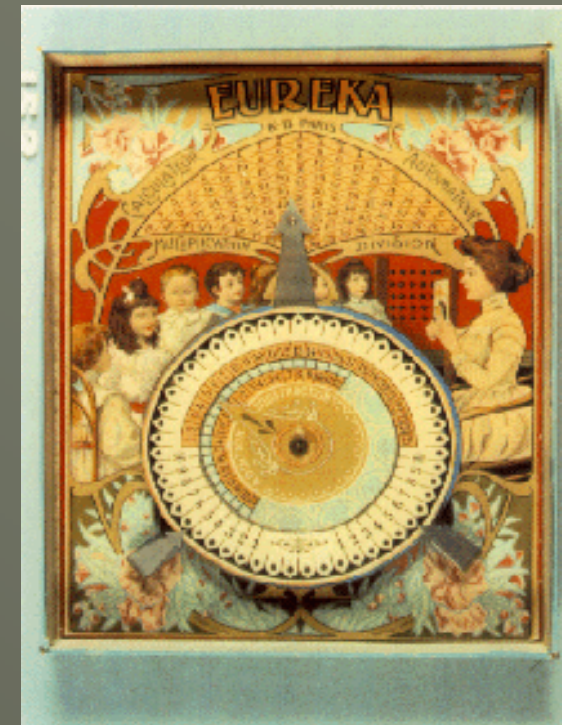
Trusted Draw™ Options

- ◆ Multiple and non-standard games
- ◆ GPS Time synchronization
- ◆ Multiple LYNKS cards for redundancy
- ◆ Multiple drawing PCs / multiple site environments
- ◆ Customized interfaces
- ◆ Customized graphics
- ◆ Interfacing with other vendors graphics applications

The screenshot displays a Lotto draw interface. At the top left, it says "Lotto". In the center, a grid of 49 numbered balls is shown. To the right, the date and time are "September 2, 2003 13:02:45". Below the date is the Sprint logo and a woman holding a mobile phone. A timer indicates "NEXT DRAW IN: 0:15". At the bottom, the draw details are "DRAW 723 13:02:00" with additional information: "Δ: -03 sequence #: 000441 signature: xxxxxx 5a2929". The winning numbers are displayed in large boxes: 3, 12, 25, 29, 37, 44. The Szrek2Solutions logo is visible in the bottom right corner of the interface.

Trusted Play™

Innovative Secure System for
'Instantaneous Winners'



- ◆ Applications: Internet betting, traditional lottery, video lottery, casino machines, mobile betting, ...
- ◆ Assures random and fair selection for a desired distribution
- ◆ "Instantaneous" winner selection product that provides system integrity, eliminating risk of fraud
- ◆ Integrity provable to vendors, game providers and auditors
- ◆ Any attempt of fraud detected by audit procedures
- ◆ Uses 'U-RAN' (Unpredictable Random Auditable Numbers), our patent-pending method, to provide ultimate security
- ◆ Utilizes cryptographic hardware and digital signature technology
- ◆ Can be integrated with 3rd party systems or provided as service

Demo

Szrek2Solutions

November 30, 2003 11:26:17

DRAW 0627 November 30, 2003 11:26:00

5 8 25 33 39

Copyright © 2003 Szrek2Solutions

November 30, 2003 10:17:03

DRAW 0558 November 30, 2003 10:17:00

0 4 16 28 32 36

Copyright © 2003 Szrek2Solutions

KENO

November 30, 2003 22:11:29

NEXT DRAW IN:
0:30

DRAW 1332 November 30, 2003 22:11:00

9	12	13	14	16	19	23	24	25	28
37	43	44	47	50	53	54	57	62	74

Copyright © 2003 Szrek2Solutions

November 30, 2003 18:28:08

NEXT DRAW IN:
0:51

DRAW 1049 November 30, 2003 18:28:00

4 5 16 28 32 36

Copyright © 2003 Szrek2Solutions

Szrek2Solutions does not provide Trusted Draw™ to Massachusetts Lottery. Sample games and logos are used with Massachusetts Lottery permission.

December 4, 2003

Confidential and Proprietary

© Szrek2Solutions

Requirements



- Draw outcomes can **not** be **predictable**
 - Generated draw outcomes have to meet **desired statistical properties**
 - The generated draw **outcomes**, actual numbers drawn, have to be **provably secure**
 - The **process** and time of generation of draw outcomes has to be also provably **secure**
 - Each draw outcome generation has to be **accounted for**
-
- Easy to use **verification functionality** for draw outcomes should exist
 - There should be **no proprietary hardware or algorithms** used to ensure security
 - **Tamper evident or tamper proof hardware** should protect critical information - **no secrets** that could be exposed
 - System must be **resilient against attacks**