Trusted Draw™ - Secure Computerized Drawing System

Abstract

For the last few years lotteries have been introducing computerized drawing machines to reduce[i] cost and provide draws for new games with frequent draws. Computerized drawing machines used currently are vulnerable to insider attacks. In this article we present the Trusted Draw™, secure computerized drawing system, with audit capability, using modern cryptographic hardware and software. Numbers drawn are unpredictable and have desired statistical properties[ii]. Audit verifies draw time and unequivocally verifies numbers drawn. Audit certifies that there was no fraud during the draw process. This solution is designed to detect insider attacks; even years after the draws are held. Trusted Draw™ is based on a patented method of generating Random Unpredictable Numbers w/Audit (RUN-A) and securing electronic draw.

Introduction

Security and integrity of the draw data, drawing equipment and drawing process is one of the most critical elements for conducting games of chance. Over the years the lottery industry saw many issues related to manipulating outcomes of mechanical drawing devices. Similar tampering attempts should be expected against computerized drawing equipment. The problem facing the gaming industry is not how to generate random numbers, but how to do it securely, in an auditable fashion. Any publicized case of defrauding computerized drawing machines could have a disastrous effect on the whole industry as they currently all have a very limited audit capability[iii]. Electronic drawing machines are exposed to many security threats from the environment they are in. Even if the machine is supervised in a locked room, protected by a special enclosure, connected using a private network and a custom protocol, the environment could be insecure.

Security Threats Against Computerized Draws

Some of the threats are listed below [2]:

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.
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 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 the attacker to predetermine the draw numbers. The same input data for randomizer may produce the same random. Attacker may know the input ahead of time and predict the numbers drawn…
7. **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 the drawing process may be compromised.
8. **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.
9. **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.
10. **Fishing**: draw numbers are requested multiple times, attacker chooses 'suitable' draw numbers.
11. **Ignoring drawing machine results**. Gaming software may be manipulated to produce its own draw numbers and simply ignore drawing machine results.

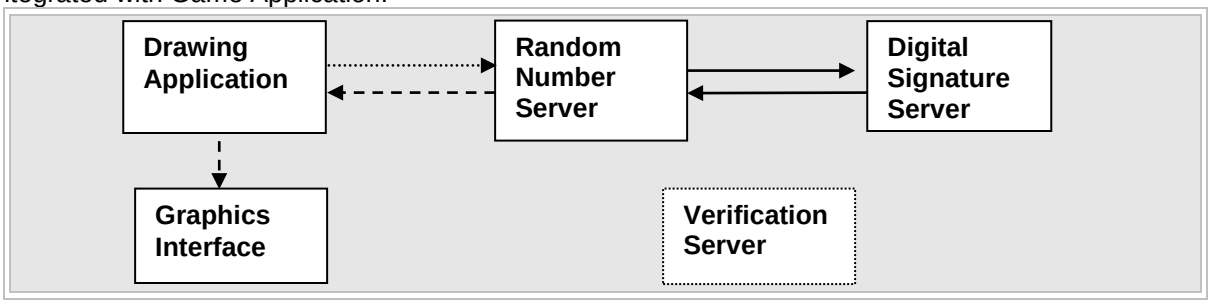
Given all these threats, how can we safely protect computerized drawing systems from insider fraud?[iv] Assuming that a skilled attacker has all possible tools to attack the drawing system: access to software, hardware, any information or algorithms stored in the drawing device, means to change any code , can integrity of the draw be preserved and any attempts at tampering with the drawing equipment be detected? Surprisingly, the answer is YES. Trusted Draw™ can provide a provably secure environment for computerized drawing.

Fcerti

Trusted Draw™ System

Below we present Trusted Draw™ system [3]. It is an electronic drawing system producing secure and auditable draw results for games of chance, supporting multiple methods for draw data generation and verification. It is specially designed to protect draws against insider fraud via use of state of the art cryptographic hardware and software[v]. Trusted Draw™ provides ultimate computerized draw security and verifiable integrity at a low cost. The main advantage of using Trusted Draw™ over any other draw system is its audit capability which allows to detect insider fraud. The audit of the draw results proves the integrity of the draws; even years after the draws are held. Trusted Draw provides most effective and conclusive tamper detection solutions.

Trusted Draw™ system consists of a PC based Random Number Server, a Digital Signature Server with incorruptible RTC (Real Time Clock), a Verification Server and a Graphics Interface. Drawing Application uses Random Number Server for draw numbers generation. It is either PC based or its functionality is integrated with Game Application.



The following describes draw numbers generation and a verification process:

1. **Drawing Application requests draw numbers** from the Random Number Server. It passes to Random Number Server information such as game identifier, draw no, etc.
2. Random Number Server provides user data to the Digital Signature Server.
3. **Digital Signature Server** is a cryptographic tamper evident device – it **combines user data with RTC to obtain digital signature.**
4. **Random Number Server uses elements of this signature for random numbers generation to produce draw data.** Random Number Server logs relevant data for audit.
5. Random Number Server passes draw numbers back to Drawing Application.
6. Drawing Application passes numbers drawn to Graphical Interface for display.
7. The Verification Server uses logged data for auditing (drawing application data, digital signatures, RTC), recreates generated numbers drawn and uses the outcome to verify the numbers drawn and time of the draw. Verification Server is an independent PC. Its functionality could also be integrated into Lottery ICS (Internal Control System).

Security Elements

There are many elements making this process secure and tamper evident against the fraud:

1. Digital Signature Server is based on cryptographic Hardware Security Module (HSM)[vi]:
    a. **HSM used is tamper evident**: secret data cannot be retrieved without destroying Digital Signature Server.
    b. **Cryptographic processor generates a unique cryptographic key pair**: private (secret) key and public (verification) key. **Private key is kept secret and never available outside cryptographic hardware**, even during its generation. Public key is delivered to the Verification Server.
    c. Digital Signature Server has a built-in **incorruptible battery backed-up Real Time Clock** (RTC). **Both user data and RTC are signed (time-stamped).**
    d. Additional features of cryptographic hardware ensure integrity for gaming applications [5].
2. **Digital signatures (without the knowledge of private key) are not predictable and have**

random characteristics. Because of this unpredictability, **digital signatures** are a good **source of randomness** and are used for the generation of draw numbers [5]. Generated random numbers have **cryptographic strength of 1024 bit RSA digital signatures**, which means they should not be breakable during the next 20 years.

3. The only "secret" element in the whole process is a private (secret) key. Without its knowledge one cannot generate drawn numbers, however one can still verify them using a public (verification) key. **The secrecy of the private key is protected by the tamper evident HSM.**
4. The method used for generating the draw numbers avoids any random number generation bias [5]. Generated numbers drawn were verified to have **good statistical properties**.[vii]
5. There is **no secret or proprietary algorithm or other secret data** used in the drawing process that could be exposed and could compromise the drawing.
6. **Only field proven hardware solutions and standard publicly scrutinized cryptographic algorithms and methods are used.** This ensures that any weaknesses of private algorithms, methods, or specialized hardware are avoided.
7. **Audit/verification can be done any time after the draw**, even a few years later. It consists of:
    a. **Authentication of the Drawing Device** – public (verification) key always authenticates drawing device as private/public key pair is unique.
    b. **Drawn numbers audit** – by checking the digital signature and recreating the numbers drawn, drawn numbers are verified.
    c. **Draw time audit** – incorruptible Real Time Clock is also signed. RTC is compared against expected draw time and verified.
    d. **Game matrix audit** – game matrix (e.g. 6 of 49) is used in the recreation of the draw numbers; if the game matrix were changed, numbers drawn would not verify.
    e. **Superfluous or missing draw detection** – additional techniques were used to detect missing draws or extra draw numbers generation.

Conclusion

Trusted Draw™ provides unique technology for electronic draws, designed to protect against fraud. It can be used for drawing for most games of chance: lotto, keno, bingo, numbers, raffle, second chance, card games. It provides provable security for the draw using digital signatures, time stamping and modern cryptographic hardware and software. The numbers drawn are unpredictable and have desired statistical properties. The audit capability is unique and essential – it verifies the draw time and numbers drawn; it certifies the draw integrity. By introducing the Trusted Draw™ electronic draw system lotteries will significantly lower the risk of attack against computerized draws, as any such attack would be detected. Should an attack still take place, Trusted Draw™ audit subsystem will provide all necessary data to identify the tampered elements. Due to use of digital signature the evidence provided by Trusted Draw and audit is admissible at court of law.

Product Feature Comparison	Legacy Solution	Trusted Draw™
Generates instantaneous draw results with the desired distribution	YES	YES
Generates random draw results with good auditable statistical properties	YES	YES
Audit can always determine whether the draw was compromised	NO	YES
Verifiable integrity and security for a non-secure environment	NO	YES
Time of generation of winning numbers is auditable	NO	YES
All information leading to the draw outcome can be published for an independent verification	NO	YES
Resistant against the insider attack	NO	YES
Single master journal file provided for the audit	NO	YES

Product Feature Comparison (continued)	Legacy Solution	Trusted Draw™
Reliance on publicly available components and standards rather then internal secret data or proprietary algorithm that could be exposed	NO	YES
No possibility to access or to compromise sensitive data by internal or external user, or auditor	NO	YES
Low cost of audit	NO	YES
Tamper proof / tamper evident draw security	NO	YES

References

[1] "Computer Generated Draws: An International View" – Public Gaming International, November 2002.http://www.publicgaming.org/pubgammag.html
[2] "Electronic Drawing Machines – Security threats" – Szrek2Solutions – www.szrek.com
[3] "Trusted Draw™ - technical specifications" – Szrek2Solutions – www.szrek.com
[4] "RFC 1750 – Randomness Recommendations for Security." www.faqs.org/rfcs/rfc1750.html
[5] "Szrek2Solutions Trusted Product Evaluation: Unpredictable and Auditable Random Number Generation for use in Gaming Applications" – Russ Housley, Vigil Security LLC. Report VS-2003-01
[6]] "The Minnesota Lottery's New Digital Draw Show Debut" - Lottery Insider, vol.22,, http://www.lotteryinsider.com.au/

[i] Lottery Insider, vol.22, in 'The Minnesota Lottery's New Digital Draw Show Debut' states:'…The Minnesota Lottery expects to save $600,000 a year by changing the studio and television to computerized drawings which is the direction many lotteries are going to in order to return more profits to their states' coffers. ``It's cheaper and, we think, more entertaining,'' said Andersen. More than a third of the nation's state lotteries use some type of "random number generator" to select winning draw numbers to save time and money in conducting draws'.
[ii] Random properties of Trusted Draw have been certified by numerous authorities and labs in the US and in Europe.
[iii] In SAZKA a.s. "every Keno draw is subject to analysis compared to all other draws for a range of statistical tests" [1]. These kinds of tests do not detect any fraud; they only determine that the numbers drawn look random. These tests are very important; however they serve only to protect the lottery against defects in draw numbers generation software that could be exploited by players.
[iv] According to most statistics over 80% of computer related crime is committed by insiders.
[v] Digital Signature is a method of signing digital data. A signer generates a pair of asymmetric keys: private and public. The signer keeps private key secret and publishes public key. To sign a document, signer uses private key. The signature can be verified using a public key from the pair. One such key pair is used to sign and verify many documents. Digital Signatures technology is not new in the Lottery environment. E.g. it is used by the Lottery in Saxony, Germany, to protect the transaction data file.
[vi] Trusted Draw™ works with LYNKS Privacy Card – a plug-in digital signature device by SPYRUS, world's largest producer of PC Card based security tokens. LYNKS Privacy Card is a tamper evident PCMCIA device. It keeps its private key in the CMOS memory not accessible externally. LYNKS Privacy Card is Federal Information Processing Standard (FIPS) 140-1 level 2 certified (tamper evident). This card is used by many commercial companies and governmental agencies. SPYRUS upgraded card firmware to ensure integrity for gaming applications. http://www.spyrus.com/content/products/rosetta/HSM.asp
[vii] Trusted Draw™ went through very rigorous statistical tests: chi square of repeated numbers, chi square of repeated combinations of numbers, and 'Diehard Battery of Tests' (http://stat.fsu.edu/~geo/diehard.html) Diehard is a battery of tests for random number generators developed by Dr. George Marsaglia of Florida State University Department of Statistics. Originally developed for testing pseudo-random generators, Diehard has since become a de facto standard for testing RNG-s.