Trusted Audit™

Summary

Trusted Audit™ (TA) is an integral part of the Trusted Product Suite. The main function of TA is to verify the integrity of draws, games, tickets, and transactions processed by the other trusted products. The RNG method[1] used by trusted products provides *nonrepudiation* - undeniable proof of integrity for each generated random number it provides, including the values of the outcomes and all associated game data (such as the game matrix, player id, hash of wagers, etc.). This proof of integrity is verified by TA.

Sample Problems Detected by Trusted Audit

Malfunctions of the draw system: Problems with repeat draw results related to draw system malfunctions will not happen on the Trusted Draw system since such problems would be detected *prior to* the Trusted Draw system generating the random numbers. Additionally, Trusted Audit independently detects the RNG system malfunction.

Manipulation of the draw results: Trusted Audit detects any and all kinds of draw results manipulations when Trusted Draw and Trusted Audit are deployed. In a recent case of the manipulation of the MUSL system (provide the link), draw systems in multiple lotteries were defrauded for many years without detection, and the fraud was only caught by accident. Trusted Audit would detect the first attempt to defraud the draw system. If the Lottery wanted to go back to every draw since inception and prove or disprove its integrity, this process would take a few days instead of many years of investigative work.

Confirming draw integrity for any draw: Sometimes draw results may turn out to be identical on proximate draws or someone may perceive a pattern in the draw outcomes, or any event can occur which causes people to question the fairness of the draw. In this case and for any other draw in which proof is desired, Trusted Audit can prove system integrity and assure that these were legitimate random events.

Deployment

Trusted Audit can be deployed in multiple configurations: as a standalone air gapped system, connected to a remote draw system, or connected to a gaming system in an integrated online environment. TA can be operated manually via a local or remote Graphical User Interface or it can be automated. Trusted Audit can also be integrated with an ICS system for real time draw outcomes verification. In addition, Trusted Audit can be provided as a service by Szrek.

Integrity of the RNG Outcomes

TA performs a verification function for the trusted products using proof of integrity generated with every transaction. More specifically, TA receives a tamper proof data file from one of the other products - a Signature File - which includes a nonrepudiation record

[1] The method of generating random numbers is protected by Szrek's patents (US patent no 6,934,846, and other international patents).

for each generated random number. The Signature File is used to verify the integrity of random number generation and to confirm that RNG hardware worked correctly. TA verifies the RNG seed and recreates all random numbers generated on the RNG platform.[2] If the RNG seed proves to be correct and random numbers match the original numbers then TA guarantees that:

- RNG hardware and software were intact (no failure or glitches)
- Electronic drawing results and instant game outcomes were not manipulated
- All generated random numbers are accounted for
- Generation followed the proper game rules, results were drawn from the correct matrix

In online environments TA provides additional control facilities for the gaming system:

- Proof of integrity of wager transactions or tickets, i.e. wagers were not manipulated after the draw
- Proof of player ids for instant games links players to instant game outcomes.
- Automation of the verification process when integrated with ICS

Legal Proof of Integrity

The Signature File which is created by Trusted Draw and analyzed by TA can provide proof in the court of law in most countries. Such proof can be useful in different situations. When draws are correct and valid, the Signature File can be used in court to prove the validity of any questionable draws. On the other hand, if there is fraud, it will be detected by Trusted Audit, and the Signature File can be used in court as evidence against perpetrators.

Reviews

Multiple technical labs, including Delehanty Consulting/SeNet, Eclipse Testing, and Bulletproof/GLI, have reviewed Trusted Audit and its ability to verify the integrity of RNG outcomes. We can provide details of these assessments on an individual basis.

[2] Random numbers are generated from the RNG seed. The digital signature, used as the RNG seed, is generated using a secret private key. The signature (RNG seed) verification is done using a public key and it proves there were no faults in the RNG hardware. Trusted Draw uses a NIST certified Hardware Security Module (HSM) to protect digital signatures/the RNG seed generation process.