Government-Run Internet Gaming Systems

TR 98-39
October 15, 1998

Bruce Schneier, Alex Igelman, and John Kelsey

1. EXECUTIVE SUMMARY

(a) In this document, we discuss the cryptographic and security requirements of a government-run Internet gaming system (called a "**casino**.").

(b) The main advantage of a casino run by a trustworthy entity such as a government is that potential customers may be brought in by the lower likelihood of getting cheated and the well-defined mechanisms for dispute resolution.

(c) The main disadvantage of a government-run casino is that, in taking measures to refuse access to children and compulsive gamblers, the casino makes access less convenient for all users, especially those overseas.

(d) Cryptography can be used in various ways to prevent cheating by users and by rogue casino employees. It can also make dispute resolution much more straightforward.

(e) Along with cryptography, good administrative procedures for resolving disputes (most will probably be caused by communications failures) will enhance the government-run casino's reputation over time. By contrast, offshore casinos may not have any way of resolving disputes other than by telling the angry customer to go away.

(f) To prevent children and compulsive gamblers from using the government-run casino, customers will have to be issued IDs of some kind, probably implemented as cryptographic certificates.

(g) Access to the names and financial arrangements of the customers must be very closely held. Various kinds of criminals would find this data very useful for planning robberies, kidnappings, con games, a c.

(h) Some problems cannot be solved by this kind of system. The availability of a government-run casino will certainly not prevent children or compulsive gamblers from seeking other Internet casinos that don't have the same kinds of restrictions on use. Similarly, daily loss limits, restrictions on kinds of games, etc., may be bypassed on the Internet.

2. INTRODUCTION

Internet casinos and gambling have become big business in the last couple of years. By setting up casinos on the Internet, casino operators get very low operating costs, and get to set up their casinos in a lax regulatory environment. Many customers connect to these casinos from places where gambling is illegal, or where casinos are set up only by a small number of favored operators.

The downside of the laxness of regulations for the casinos and players is obvious: These are typically low-budget operations that are fairly new; there aren't a lot of Internet casinos with good reputations yet. Many of these casinos are likely to defraud their customers; honest casinos aren't likely to be trusted by their customers.

A large part of the task of keeping everyone honest can be accomplished by use of cryptographic methods: Random events like card shuffles and die rolls can be made unpredictable to both player and casino; well- defined legal or administrative remedies can be made available to resolve disputes; be ions of each party can be entered into very hard-to-forge, hard-to-erase logs, to be retrieved if there is a dispute between them; users can be issued certificates verifying that, according to the best information available to the government's records, they are neither children nor compulsive gamblers.

Users may find that a government-run casino, with well-defined dispute resolution mechanisms and a good reputation is preferable to an offshore Internet casino, which may cheat or refuse to pay of n some large wins. Additionally, the government-run casino can adhere to data privacy laws and other restrictions to prevent the names and addresses of known gamblers from being sold. Offshore casinos will likely be less trustworthy; whatever promises they make about reselling data will be less credible.

The following are the intended goals, as we see them:

(a) Set up a government-run Internet casino.

(b) Set up a system of digital IDs so that children, the mentally incompetent, and compulsive gamblers cannot use this casino. Somehow link this ID with the payment mechanism used.

(c) Ensure that any one person has a hard time getting more than one ID. Use this property to enforce daily loss limits in this casino.

(d) Use cryptographic methods to ensure that all games are fair. In this system, this mainly means resisting the efforts of rogue casino employees to cheat.

(e) Use cryptographic logging and digital signatures, along with the correct administrative structure, to allow a well-understood and fair mechanism for resolving disputes between this casino and its users.

It is important to note the problems which this system cannot solve. These include:

(f) Children, compulsive gamblers, and the mentally incompetent will still be able to gamble at other Internet casinos not run by the government. It seems unlikely that the government will successfully prevent citizens from gaining access to these casinos without tightly regulating Internet access.

(g) Gamblers will always be able to lose their whole daily loss limit at the government-run casino, and then go to another Internet casino outside the country and lose more.

(h) Lists of known gamblers, compulsive gamblers, and players who have recently won a large amount of money are all collected under this system. These lists would be valuable to a variety of criminals. While we can put administrative mechanisms in place to prevent their getting these lists, we can't guarantee they won't be sold by some rogue employee.

3. IDENTIFYING USERS

Each user is required to go through some kind of registration process before playing at the casino. This is used to guarantee that each person can have only one ID active at a time, and to ensure that no children or known compulsive gamblers can use this casino. User IDs can be tied to physical address, taxpayer number, name, etc. They are never issued to compulsive gamblers or children. People may also ask to be entered onto a list that will never have such an ID made for them. Governments have a number of mechanisms for verifying identification; we assume some such method will be used here.

The ID will consist of a certificate for this user's account number. The account number will then be linked in some database with a payment method. The casino's mechanisms for accepting and paying out money should be designed so that no employee who has access to the account numbers also has access to the payment records, which would probably allow them to learn users' identities.

Note that whatever payment mechanism is used, if it keeps track of the names of its users (as a credit card does, for example), those names should be verified against the name in the database for this ID. Additionally, large payouts should be done in some more secure way, perhaps by visiting the home of the owner of the ID by private courier, bringing a cashier's check.

The IDs are regular certificates, meaning they can be revoked. A list of revoked certificates will be kept available to the Internet casino.

Any special software required by the user will be provided to him at the time his ID is granted.

Note that there must be some way to keep people from giving their IDs away or selling them. We recommend tying the ID loosely into the payment mechanism used. The operations of the games should be administratively separated from the payments in and out. The casino should only pay out to accounts in the same name as the ID is in; it may also refuse to accept payments in from accounts in any other name. Additionally, there may need to be legal action taken against people found giving their IDs away or selling them.

4. VERIFYING GAMING SOFTWARE

Casino and player software needs to be reviewed carefully to make certain that a rogue employee hasn't placed some kind of back door into them. Cryptographic protocols can make some kinds of cheating hard for an attacker with control over one piece of software or another; an attacker with control of both pieces of software will be able to cheat.

Fortunately, by giving a computer to the players, and by careful use of cryptography, it is possible to prevent most of the simple kinds of cheating that an attacker might try. The electronic equivalent of "loaded dice" are fairly easy to prevent, simply by having both the player and the casino software generate a random number, and then adding the two numbers together. The result is a random number not under the control of either party (Note that this is a slight oversimplification) (the addition has to be done in such a way that the result falls into the same range, with the same uniform distribution, as the original random number). As a simple example, if Alice and Bob each have coins, they can accomplish a fair coin toss if either of them has a fair coin; they agree that Alice will win the toss if both coins are the same, and Bob will win if they are different. The reader can satisfy himself that this will produce a fair outcome if either coin is fair, even if the other coin has two heads.

4.1 Player Software

We expect some player software to be necessary to make it hard for casino employees to cheat. Since the customer is likely going to be connecting to the casino with a web browser, we expect this player software to be written in Java and to be digitally signed by the casino. Player software needs to be closely reviewed, and also needs to be kept as simple as possible. This player software may need to be available for instant download at the casino's web page. Player software should be involved in the following actions:

(a) Each time a random number is to be generated and used, the player software should generate its own random number and verify that it is used along with the casino's number.

(b) Each time any important financial or game event happens (such as the placing of a wager, the dealing of a card, paying off from a winning game, etc.), this should be added to the player's audit log file.

(c) The audit log should be restarted every so often by connecting to a server under the control of the casino. This should be handled by the player software. (The part of the casino's staff that controls the log server should not also be involved in writing, maintaining, or using the actual gaming software.)

(d) The audit log for a play of a game must be submitted by both player and the gaming part of the casino to the payout part of the casino. The casino should refuse to pay out unless the logs are in order. Note that payout and playing need to be administratively separate; nobody should have access to software or hardware for both.

The player software will probably be different for different sets of games offered, so that it can audit each game's important events intelligently, and so that it can properly take part in generating shared random numbers. There are a great many important issues regarding the performance of the player software that need to be worked out, particularly involving the generation of good unpredictable numbers.

5. RANDOM EVENTS AND INTERNET GAMBLING

5.1 General Principles

(a) Gambling only works where there is unpredictability. Using cryptography, it is possible for the player and the casino to each be certain that the other isn't cheating them.

(b) Generating unpredictable (pseudo-random) values on a deterministic machine like a computer is a demanding task. We can help select methods to recommend or require, possibly including the use of specialized hardware.

(c) It is possible, using deterministic methods to generate unpredictable values during each gaming session, to make auditable the pseudo-random sequences generated by the casino and the player. The casino can commit to the pseudo-random seed used in the logs before the game begins, in some public way. The player, and any court called upon to resolve a dispute, can now verify whether the random numbers were generated according to the required mechanism.

5.2 Using Cryptography to Make the Game Fair

Cryptography provides powerful tools for allowing two different parties who don't trust one another to mutually generate numbers that are unpredictable to either party. Making use of this in Internet casinos means that the electronic equivalent of loaded dice, or two-headed coins, simply doesn't work. This radically reduces the risk of cheating by rogue employees at the casino.

Without going into great detail, the basic method for two parties (we will refer to the parties as Alice and Bob, to make the description more readable) to generate a number unpredictable to either one is as follows:

(a) Alice generates a random number, RO , and commits to it. For now, think of this as writing it down and sealing it into an envelope, and then giving it to Bob.

(b) Bob generates a random number, R1 . He gives it to Alice.

(c) Bob opens the envelope from Alice. He computes RO + R1 . Alice also computes RO + R1 .

(d) Alice and Bob now both share this number, which is not under the control of either of them.

More elaborate cryptographic methods have been designed for all sorts of things, including shuffling cards. This can be put into the player software. If for some reason player software can't be used, there are other alternatives, although they do complicate the design somewhat.

5.3 Sources of Random and Pseudo-Random Numbers

There are well-understood cryptographic mechanisms that, given a secret starting point, will generate a huge number of unpredictable numbers. That is, an observer who doesn't know that starting point can see a huge number of numbers, and still have no way to predict what the next number will be. In modern cryptographic software, the biggest problem tends to be finding such a secret starting point, and recovering a new secret starting point if the currently used one is discovered somehow.

Computers are deterministic machines, and they don't usually have alot of unpredictable things going on inside. Unpredictable inputs usually come from interactions with users or other machines over a network, from "noisy" physical processes like the time taken by hard drive reads and writes, or from specialized hardware designed to generate random numbers from physical phenomena, such as thermal noise in electric circuits.

We will probably recommend that the casino make use of special-purpose hardware for generating random numbers. The casino machines can use these random numbers to reset the starting point of the cryptographic mechanism being used to generate unpredictable numbers.

Player software will probably maintain a file containing hard-to-guess numbers on the user's machine. Each time the player software is started, it will use this file for its starting point, and try to slowly accumulate unpredictable values from user interactions, disk read times, etc.

We will likely recommend the use of some well-known cryptographic mechanism, such as SHA1 in counter-mode or triple-DES in OFB-mode, for generating the unpredictable values.

All the above comments are very preliminary; we will need to know a great deal more about the requirements of these systems before we can make solid design recommendations.

5.4 Auditable Pseudo-Random Numbers

To prevent rogue employees and users from conspiring to win money unfairly, we can make use of auditable random numbers. In this case, we have a tamper-resistant module on the casino machine which must be used to get random numbers for the casino's part of the cryptographic protocols. Each output random number is signed and time stamped by the token. The casino software supplies all the signed and time stamped random numbers to the user when he wins; these are then presented as part of a claim of a winning. An administratively different part of the casino controls this process, and it verifies all the signatures in the block to guarantee that the casino software behaved as it should have.

6. RESOLVING DISPUTES VIA PASSIVE LOGGING

6.1 General Principles

(a) Casinos and players each log all interactions. In particular, all payout-relevant actions should be logged. This makes recovering from disputes and communications failures easy.

(b) Digital signatures should be used to provide nonrepudiation in logs at each really critical point. That is, at each critical point, both the casino and the player digitally sign some statement of what they're trying to do.

6.2 Audit Logs

Counterpane Systems has developed cryptographic audit logging technology, which makes it possible for the logging machine to enter data into logs, which it cannot subsequently read or change. Another machine, in this case one under the control of a different part of the casino, is able to read and verify these logs.

6.3 Non-Repudiation

During any interaction between the casino and the player, the parties can exchange digitally signed commitments to their current values, and then enter these into their logs. The result is proof of the actions of one another, kept in log files to be produced if a dispute arises. We can discuss this in greater detail as needed; for now, accept that we can get the equivalent of signatures and countersignatures from the player and casino on each roll of the dice or shuffle of the cards, and each bet placed, if we need it.

6.4 Resolving Disputes

One advantage of having a casino in a real legal jurisdiction with courts with some reputation for fairness is that disputes between the casino and players will have some real dispute-resolution mechanism. A dispute is really any situation in which one party feels that the other has behaved unfairly; the most obvious case might be when the user has won a gamble but the casino has refused to pay him. In practice, we expect the most common disputes to be about communications failures.

7. OTHER CONCERNS AND COMMENTS

7.1 Overview

(a) Privacy issues probably need to be addressed somewhere in the design process. It takes no imagination at all to come up with a number of bad things that could happen, if a really unethical person were given access to a list of names, addresses, and credit card numbers of heavy gamblers.

(b) Detecting minors and compulsive gamblers is just hard. Issuing IDs for approved gamblers is expensive, and may lead some legitimate users to go to another casino where there's not so much hassle to be allowed to play.

(c) Lots of countries, including the U.S., seem to be taking an approach of making Internet gambling illegal. Others are looking at them as cash cows, and letting them run without concern about fraud. If some responsible government manages to run an Internet casino to protect customers from fraud, that casino may find that they get business from all over the world; gamblers probably don't want to get ripped off any more than anyone else. The ID mechanism needs to be designed with these international users in mind.

7.2 Privacy Issues

There are several sets of privacy issues to be dealt with here:

(a) *Customer Identity Privacy* Customers of the casino must have their identities remain private. This should be done by separating out administrative access to the full ID records, which include identifying information, and the ID records used by the casino gaming software, which have no direct identifying information. It is especially important not to let the list of known compulsive gamblers be sold. Perhaps the one-way hashes of those people's legal names could be stored at the casino somewhere;

this would allow checking to see if a name was on the list, but not easy retrieval of the whole list's contents.

(b) *Customer Financial Privacy* Customers should also have their financial privacy protected. It is important that nobody be able to accumulate a listing of big recent winners or gamblers, since that would amount to a list of good people to attempt to rob or blackmail. The casino will have the ability to build such a list, but obviously shouldn't do so.

Note that in all these cases, privacy depends upon the discretion of the casino's employees, as well as on its policies. Cryptography, computer security, and physical security can only do so much to help; the main issue is the integrity of those people. Presumably, casinos already have considerable experience in dealing with this kind of issue.

7.3 Keeping Out Children and Compulsive Gamblers

There are some people who should be kept away from any kind of gambling. Among these are children, compulsive gamblers, and the mentally incompetent. In this system, we use a single government-issued credential to verify age and eligibility to play. This has the cost that it is somewhat time-consuming to sign up. However, it will largely keep children and compulsive gamblers out of the online casino.

Note that if such IDs are issued only within one country, then the casino must either refuse all international business, or must try to differentiate between people connecting from inside or outside the country. This won't be too hard to evade, but still might be worthwhile.

A second alternative, which should probably be combined with the IDs, is to use existing content-rating services on the web. That is, the casino can specify ratings of "adults only," keeping children out if their parents have installed some kind of content-filtering program on their web browser.

The most important thing to realize about this is that it is much harder to stop compulsive gamblers and (to a lesser extent) children from getting access to online casinos than from getting access to real-world casinos. There are no ideal solutions for this problem. We can probably keep them out of the government-run Internet casinos, but not others out somewhere on the net.

8. SUMMARY AND CONCLUSIONS

In this document, we have discussed how an Internet casino might be run by a government. We believe that both the casino and the players will need to use specially designed and reviewed software to gamble safely. We recommend spending considerable time and effort on ensuring that both players and the casino have access to unpredictable numbers on demand, as well as on designing cryptographic protocols to ensure that the games can't be cheated in by either the casino or the player. We recommend the use of extensive audit logs on both the casino and the player, so that disputes between them may be resolved; we have designed audit logging techniques that will be especially useful in this application.