

Il falsario contro il crittologo: sicurezza per la lotteria informatizzata

*The Forger vs. the Cryptologist:
Security Issues for the Computerised Lottery*

Francesco Stajano
AT&T Laboratories Cambridge
<http://www.uk.research.att.com/~fms/>
University of Cambridge Computer Laboratory
<http://www.cl.cam.ac.uk/~fms27/>

Abstract: We present the main security issues for a lottery system using a hypothetical sequence of attacks, defenses and counterattacks. Cryptologic techniques are introduced where appropriate and the case of a fully digital lottery scenario is also examined.

1. Scenario

Lo scopo di questo intervento è di illustrare il problema della sicurezza per una lotteria informatizzata e di mostrare in quali circostanze e con quali modalità la crittologia possa offrire valide soluzioni.

Per impostare il problema definiamo anzitutto un modello semplificato del sistema lotteria. I protagonisti sono il banco ed i suoi clienti. Ogni cliente può, dietro pagamento di una somma, scommettere contro il banco sull'esito di un predeterminato evento futuro. Alla scadenza prestabilita il banco chiude i giochi, ossia cessa di accettare scommesse. Dopo un certo intervallo di tempo l'evento ha luogo e, a quel punto, il banco paga un premio ai clienti le cui previsioni si sono verificate.

Le frodi identificabili a questo livello di astrazione sono essenzialmente di due tipi: scommettere quando l'esito dell'evento è già noto oppure influenzare l'evento in modo da rendere alcuni esiti più probabili di quanto non fossero a priori. La frode del secondo tipo è particolarmente interessante in quanto avviene totalmente al di fuori delle interazioni fra il cliente e la lotteria e richiede contromisure più legali che crittologiche. Il grave errore sarebbe omettere di considerarla nell'analisi di sicurezza illudendosi che "questo non spetta a noi".

Torniamo al modello ed arricchiamolo (salto qualitativo oltre che quantitativo) con le ricevitorie. Il cliente compila un modulo in cui descrive il dettaglio della scommessa (ad esempio quali numeri prevede che vengano estratti). La ricevitoria accetta il modulo ed il corrispondente pagamento e restituisce al cliente una ricevuta "timbrata", ossia in qualche modo convalidata. La ricevitoria funge da concessionario nei confronti del banco: essa paga al banco i ricavi, trattenendo una percentuale. A estrazione avvenuta il cliente vincente esibisce la ricevuta alla ricevitoria (o al banco se la vincita è sostanziosa) che, verificatane la validità, paga il premio.

2. Attacchi e difese

Il primo attacco al quale accennavamo consiste nel contraffare a posteriori una ricevuta relativa all'esito vincente. La contraffazione può essere resa più difficile sfruttando le numerose tecniche sviluppate per la stampa di banconote (carta speciale, filigrana, inchiostri metallici, ologrammi, rilievi ecc.) Tuttavia il criminale può sempre derubare una ricevitoria e procurarsi così delle ricevute vergini ed il timbro convalidatore. Il banco può contrastare questo attacco stampando dei numeri di serie sulle ricevute vergini e tenendo traccia dei furti denunciati dalle ricevitorie: qualora una ricevuta rubata venisse presentata per ritirare un premio, il banco avvierebbe un'indagine invece di pagare.

Non bisogna però cadere nell'errore di etichettare manicheisticamente tutti i dipendenti e licenziatari della lotteria come "i buoni": se la posta in gioco è una vincita multimiliardaria, per il nostro criminale può senz'altro valere la pena aprire una ricevitoria con il preciso scopo di ottenere ricevute vergini e timbro. Il banco non può dunque assiomaticamente considerare come fidate le migliaia di ricevitorie della propria rete. È qui che entra in gioco la crittologia, uno dei principali rami della quale è lo studio di protocolli per l'interazione fra protagonisti che non si fidano completamente gli uni degli altri.

La soluzione astratta al problema consiste nell'impedire alla ricevitoria di convalidare una scommessa dopo la scadenza prestabilita per la chiusura dei giochi. Il nostro metaforico "timbro" deve dunque rifiutarsi di timbrare dopo una certa data. È senz'altro possibile implementare il "timbro" come una macchina sigillata che stampa le ricevute solo durante un periodo autorizzato; ma questo significa fidarsi dell'orologio locale della macchina, che il nostro criminale tenterà senz'altro di puntare su un altro orario. D'altronde anche una macchina priva di orologio locale e che si basasse sul segnale orario radiofonico sarebbe soggetta ad attacchi in cui questo segnale venisse distorto o contraffatto.

L'approccio crittologico trasforma il problema dal dominio degli atomi a quello dei bit: abbandoniamo i dispositivi fisici di protezione (carta speciale ecc.) in favore di algoritmi che garantiscano l'inviolabilità di sequenze di bit. Questo approccio, laddove applicabile, consente un ulteriore salto qualitativo: quello in cui tutte le operazioni, "giocate" compresa, possono essere condotte via Internet.

Un modo per impedire alla ricevitoria di convalidare ricevute dopo la scadenza è di costringerla a far certificare da un notaio, entro la scadenza, l'elenco delle ricevute emesse. Il banco paga il premio solo se la ricevuta è presente nell'elenco certificato. Sigillare l'elenco delle ricevute convalidate serve anche a prevenire un'altra tipologia di attacchi: la ricevitoria mafiosa potrebbe difatti omettere di denunciare al banco una certa porzione delle vendite, intascando dunque per esse il prezzo pieno anziché la sola percentuale. Molto peggio, essa potrebbe addirittura stampare e convalidare in anticipo le ricevute relative a tutti i possibili esiti dell'evento, garantendosi quindi la vincita, ma dichiarando di averne emesse solo una minima parte e non pagando quindi la posta relativa.

La crittologia consente di sostituire il notaio con la seguente elegante costruzione. La ricevitoria pubblica l'elenco sul proprio sito web, ne calcola lo hash¹ e pubblica

¹Una funzione hash è una specie di checksum crittografico che da un input di lunghezza ar-

questo in un annuncio economico sul giornale. La pubblicazione cartacea dello hash sigilla il file, in quanto una qualunque modifica produrrebbe uno hash diverso da quello pubblicato, cosa che chiunque potrebbe indipendentemente verificare.

Con questo schema impediamo alla ricevitoria di “timbrare” dopo la scadenza, ma non abbiamo ancora chiarificato come realizzare la versione digitale del timbro, che deve essere verificabile e difficile da contraffare. Una soluzione molto semplice prevede che la ricevitoria convalidi ogni ricevuta scrivendoci un nuovo numero casuale molto lungo. Se, come si è già stabilito, l’elenco delle ricevute emesse viene conservato e “sigillato”, una ricevuta risulterà valida solo se compare nell’elenco suddetto. Questo di per sé impedisce ai clienti di creare ricevute false. Ma anche solo cambiare a posteriori i numeri scelti su una ricevuta esistente rende la ricevuta non valida, poiché essa non corrisponderà più a quella registrata nell’elenco.

Chi rimane scoperto in questo scenario è però il cliente, il quale quando paga non ha alcuna garanzia che la ricevitoria copierà la ricevuta nell’elenco, visto che l’elenco viene sigillato solo alla chiusura dei giochi e prima di quell’istante esso può essere manipolato a volontà. La ricevitoria disonesta, d’altronde, ha tutto l’interesse ad omettere di registrare la ricevuta, giacché in tal modo essa non deve pagare il corrispettivo al banco. Nel caso limite, la ricevitoria potrebbe essere del tutto illegale e non avere alcun rapporto col banco: essa venderebbe ricevute finte, mirando non al premio ma ai soldi dei clienti, e pagherebbe di tasca propria le vincite minori, giusto per non farsi scoprire; ma sparirebbe alla chetichella non appena uno dei suoi clienti dovesse vincere una grossa somma e si vedesse rifiutare il premio dal banco.

Sarebbe legittimo, da parte del cliente, esigere in cambio del pagamento una garanzia che il banco accetterà quella scommessa come valida. A tale uopo è utile un’altra primitiva crittografica, la firma digitale². Il cliente riempie il modulo con la propria scommessa; la ricevitoria vi aggiunge un numero seriale (per poter distinguere due scommesse identiche da parte di clienti diversi) e spedisce il modulo al banco. Il banco firma il modulo e lo restituisce; e, già che c’è, si segna in diretta che quella ricevitoria gli deve il pagamento per l’emissione di un’altra ricevuta. Il cliente può immediatamente verificare la validità della firma del banco sulla propria ricevuta ed è inoltre certo che il banco non potrà in seguito negare di aver firmato.

Non entreremo in tutti i dettagli, ma questo protocollo può essere ulteriormente arricchito: ad esempio la ricevitoria può apporre la propria firma sulla ricevuta prima di spedirla al banco. Questo per evitare che un banco disonesto possa chiederle di pagare per più ricevute di quante essa non abbia effettivamente emesso (operazione adesso impossibile perché la ricevitoria pagherà solo per le ricevute per le quali il banco può esibire la firma della ricevitoria stessa).

bitraria produce un output di lunghezza fissa (dell’ordine delle centinaia di bit). La funzione è “unidirezionale” nel senso che, mentre lo hash di un input può essere calcolato in tempo lineare, è viceversa computazionalmente impossibile costruire una possibile preimmagine di un dato hash.

²La firma digitale è nata dalla crittografia a chiave pubblica. Ogni potenziale firmatario ha due chiavi collegate, una privata usata per firmare e una pubblica che chiunque può usare per verificare la firma. Firmare un documento genera una stringa di bit dipendente dalla chiave privata e dal documento, verificabile con la chiave pubblica. È computazionalmente impossibile generare la firma senza la chiave privata, e qualunque modifica al documento invalida la firma. Siccome la chiave (privata) per firmare è nota solo al firmatario, questi non può rinnegare una propria firma poiché nessun altro avrebbe potuto generare una firma valida senza la sua chiave privata.

La perfetta clonabilità dei bit dà luogo a un altro problema: nello scenario Internet, ad esempio, chiunque “veda passare” una ricevuta convalidata può rubarla. Se la ricevuta risulta vincente, sia il legittimo proprietario che gli eventuali guardoni si precipiteranno a reclamare il premio e il banco non potrà far altro che constatare che tutte queste persone hanno copie della medesima ricevuta (valida), senza che sia possibile stabilire chi ne sia il vero proprietario.

È senz’altro possibile cifrare i canali di comunicazione; ma una alternativa più robusta, invece di tentare di tenere segreta la ricevuta, è di renderla nominativa, cosicché essa sia inutilizzabile da altri che non il legittimo proprietario. Il cliente fornisce il proprio nome insieme alla selezione di esiti che costituisce la scommessa; il banco firma questo messaggio composito e la ricevuta allora porta indelebilmente il nome del beneficiario al quale l’eventuale premio andrà pagato. Il principale svantaggio è, chiaramente, la perdita dell’anonimità per il cliente.

Per ovviare anche a questo inconveniente, il cliente pensa un numero casuale lungo, che tiene segreto, e ne genera lo hash. Poi tutto procede come prima, ma il cliente fornisce questo hash in luogo del proprio nome. Al momento della presentazione della ricevuta vincente, il banco paga il premio solo se chi esibisce la ricevuta può esibire anche la preimmagine dello hash in essa contenuto, cosa che chi ha copiato la ricevuta non sarà in grado di fare.

3. Conclusioni

Abbiamo esplorato maieuticamente il problema della sicurezza per la lotteria, omettendo molti dettagli (specie circa l’efficienza e la scalabilità di alcune soluzioni) ma ipotizzando anche uno scenario completamente digitale. Il messaggio importante è che la sicurezza è una catena forte solo quanto l’anello più debole e che l’analisi va affrontata in maniera olistica. La parte più difficile è stabilire quando fermarsi: c’è sempre il rischio di aver omesso di considerare qualche altro attacco.

Come esempio di ciò osserviamo che, pur avendo esplicitamente individuato e discusso la possibilità che la ricevitoria mafiosa intenda non pagare il banco per le ricevute emesse, la soluzione finora sviluppata continua a non proteggere adeguatamente il banco. Il banco *tiene accuratamente nota* del denaro che la ricevitoria gli deve, ma ciò di per sé non impedisce a questa di sparire senza pagare. È dunque anche necessario stabilire limiti finiti per il credito disponibile alle ricevitorie.

Ringraziamento: è discutendo con Ross Anderson le bozze del brillante articolo in bibliografia che l’autore si è originariamente avvicinato al problema della lotteria.

Riferimenti bibliografici

Anderson R. (1999) “How to Cheat at the Lottery (or, Massively Parallel Requirements Engineering)”, in *Proc. Annual Computer Security Applications Conference 1999*, Phoenix AZ. <http://www.cl.cam.ac.uk/~rja14/lottery/lottery.html>

Schneier B. (1996) *Applied Cryptography*, 2nd ed. Wiley. 0-471-11709-9.