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.

in *Atti della XL Riunione Scientifica della Società Italiana di Statistica*, Firenze, 26–28 aprile 2000, pp. 771–774.