Security Part 2 1999

P7 q6
RJA

You have been hired by a company which is bidding to take over the National Lottery when Camelot's franchise expires, and your ~~task~~ responsibility is the security architecture. State the security policy and outline the mechanisms you would implement to enforce it.

Model Answer

The threat model is that attackers, possibly in cahoots with insiders, will try to place bets once the result of the draw is known. They may do this ~~either~~ by altering bet records or by forging tickets. Secondary threats are that bets will be placed that are not paid for, and that attackers might operate bogus vending stations which would pay small claims but disappear if a client won a big prize.

The security policy could be to ensure that all bets are registered online with a server which can identify each ticket uniquely by time and place of sale; ~~that each ticket correctly can be~~ and that from some cut-off time prior to the draw, the server can be secured against tampering and against the extraction of sufficient information to forge a winning ticket. There should also be inspection procedures to identify bogus vendors, and credit limits on genuine vendors.

Mechanisms: On selling a ticket, a terminal sends a transaction to the server, authenticated with a MAC computed using a terminal key. The terminal's credit limit is checked and if OK is decremented; a unique

. ticket authenticator is generated and sent to the terminal, encrypted under the terminal key. This unique authenticator could be a MAC computed with a global secret key (in which case the key might well be kept in tamper-resistant hardware) or a random string (in which case it might well be split and the two halves stored on separate server databases). The authenticator, together with ticket serial number and vendor terminal ID, is written to the ticket. When the game closes, CD copies of the sever database(s) are taken and kept by independent parties. Finally, to detect bogus vendors, the help of genuine vendors is enlisted and they are motivated by giving them each a monopoly (or share of an oligopoly) in a given area.