Your debugging code can be a security hole: Contest tickets

devblogs.microsoft.com/oldnewthing/20090723-00

July 23, 2009

Raymond Chen

Last year, the Microsoft cafeterias ran a promotion which involved scratch-off tickets and prizes ranging from a free bagel to a new Zune to free airplane tickets. But it turns out that the people who ran the contest left some debugging code behind that became a security hole. As people compared notes on what they did or didn’t win, they noticed that the tickets all looked identical save for the scratch-off area (naturally) and some tiny numbers printed in the corner of the back of the card. After some study, it became clear that all the losing tickets had a code that ended in *01*, all the tickets for a free bagel ended in *18*, and so on. If you went to the contest rules and regulations Web site, you’d find the legally mandated *odds of winning* disclosure, and the table just so happened to have *no prize* as the first item in the table and *free bagel* as the eighteenth. Further comparisons with other winning tickets confirmed that you could tell ahead of time what prize you were going to win by just looking at the last two digits of the number printed on the back of the card. This is another example of how your debugging code can be a security hole. In this case, the code printed on the backs of the cards were probably added for quality control purposes, so that the contest managers could ensure that the right number of winning tickets were printed and so that the “big ticket” prizes would be evenly distributed among the participating cafeterias.

But it also meant that everybody participating in the contest knows which are the winning tickets.