Ron Rivest
23 mars

Security of Voting Systems

Abstract:

While running an election sounds simple, it is in fact extremely challenging. Not only are there millions of voters to be authenticated and millions of votes to be carefully collected, counted, and stored, there are now millions of "voting machines" containing millions of lines of code to be evaluated for security vulnerabilities. Moreover, voting systems have a unique requirement : the voter must not be given a "receipt" that would allow them to prove how they voted to someone else otherwise the voter could be coerced or bribed into voting a certain way. This lack of receipts makes the design of secure voting system much more challenging than, say, the security of banking systems (where receipts are the norm).

We discuss some of the recent trends and innovations in voting systems, as well as some of the new requirements being placed upon voting systems in the U.S., and describe some promising directions for resolving the conflicts inherent in voting system requirements, including some approaches based on cryptography. We also describe the use of the ``Scantegrity II'' end-to-end voting system, developed by David Chaum and researchers from MIT, GWU, UMBC, Ottawa, and Waterloo, in last November's election in the city of Takoma Park, Maryland.