

Swiss House talk  
Ron Rivest

### Security in Voting (specifically Internet Voting)

Security requirements for voting system:

1. Each eligible voter shall be able to vote, at most once
2. Voter shall cast a vote free from outside pressure or coercion
3. Voting system shall accurately report results
4. Other requirements follow, such as:
  - a. Voter privacy: no one should know how an individual voter voted
  - b. Voter isolation: voter should vote in isolation from outside influences (even if the voter wishes otherwise). Note that Internet Voting (and Vote by Mail) fail the voter isolation requirement
5. There are many other voting system requirements as well

In order for election results to be believed, security properties must not only be true, but verifiably true by as many participants as possible (election officials, voters, losing candidates). "Principle of maximum verifiability"

Examples:

1. Each eligible voter shall be able to vote, at most once. Who can verify:
  - a. Who is eligible to vote in given election?
  - b. How voter demonstrated identity/eligibility? (e.g. are signature records on absentee ballots public? Should voter photo and copy of ID be public?)
  - c. Who actually voted in given election?
  - d. Whether vote was accepted as valid?
2. Voter shall cast vote free from outside pressure or coercion. Who can verify:
  - a. Voter alone when he/she is voting
  - b. Voter retained no record/receipt of how he/she voted
  - c. Voter system (including pollworkers) can not link voter's identity with their cast vote record
3. Voting system shall accurately report results. Who can verify:
  - a. Voter's choices accurately recorded by voting system? (cast as intended)
  - b. Voter's ballot included in final tally? (cast ballot assurance)
  - c. Ballot as counted is same as ballot as cast?
  - d. Tabulation software is correct, correctly installed, and gives correct result?
4. Recovery procedures, if verification fails (no time to discuss at this forum)