Thoughts On Appropriate Technologies for Voting

Ronald L. Rivest

Viterbi Professor of EECS MIT, Cambridge, MA

Princeton CITP E-voting Workshop 2012-11-01



1

We live in an age of marvelous technology: cellphones, man on the moon, the web, cars that drive themselves.



- We live in an age of marvelous technology: cellphones, man on the moon, the web, cars that drive themselves.
- Many technology wishes come true wish it, and you can have it.



- We live in an age of marvelous technology: cellphones, man on the moon, the web, cars that drive themselves.
- Many technology wishes come true wish it, and you can have it.
- Is voting being "left behind"?



- We live in an age of marvelous technology: cellphones, man on the moon, the web, cars that drive themselves.
- Many technology wishes come truewish it, and you can have it.
- Is voting being "left behind"?
- Why are many of us voting on paper ballots?



- We live in an age of marvelous technology: cellphones, man on the moon, the web, cars that drive themselves.
- Many technology wishes come truewish it, and you can have it.
- Is voting being "left behind"?
- Why are many of us voting on paper ballots?
- Why not voting, say, over the Internet?



 Voting tech has often followed other tech innovations: paper ballot, lever machine, punch card, opscan ballot, DRE, ...



- Voting tech has often followed other tech innovations: paper ballot, lever machine, punch card, opscan ballot, DRE, ...
- Technology introduces design options.



- Voting tech has often followed other tech innovations: paper ballot, lever machine, punch card, opscan ballot, DRE, ...
- ► Technology introduces *design options*.
- You don't have to take them.



- Voting tech has often followed other tech innovations: paper ballot, lever machine, punch card, opscan ballot, DRE, ...
- Technology introduces design options.
- You don't have to take them.
- Sometimes low tech is better! (esp. for security)



- Voting tech has often followed other tech innovations: paper ballot, lever machine, punch card, opscan ballot, DRE, ...
- ► Technology introduces *design options*.
- You don't have to take them.
- Sometimes low tech is better! (esp. for security)
- My students prefer chalk/blackboard to powerpoint.



- Voting tech has often followed other tech innovations: paper ballot, lever machine, punch card, opscan ballot, DRE, ...
- ► Technology introduces *design options*.
- You don't have to take them.
- Sometimes low tech is better! (esp. for security)
- My students prefer chalk/blackboard to powerpoint.
- When hiking, it may be better to carry a map than to use a GPS. (What could go wrong?)



- Voting tech has often followed other tech innovations: paper ballot, lever machine, punch card, opscan ballot, DRE, ...
- ► Technology introduces *design options*.
- You don't have to take them.
- Sometimes low tech is better! (esp. for security)
- My students prefer chalk/blackboard to powerpoint.
- When hiking, it may be better to carry a map than to use a GPS. (What could go wrong?)
- Manual car window may be safer than power window.





I offer 11 "epigrams" that may help frame the discussion...



1 A voting system must determine the winner *and* convince the losers they really lost.



1 A voting system must determine the winner *and* convince the losers they really lost.

 VS is not a "trusted party," but must justify its conclusions.



1

A voting system must determine the winner *and* convince the losers they really lost.

- VS is not a "trusted party," but must justify its conclusions.
- VS must produce credible evidence that the stated outcome is correct.



1

A voting system must determine the winner *and* convince the losers they really lost.

- VS is not a "trusted party," but must justify its conclusions.
- VS must produce credible evidence that the stated outcome is correct.
- Key question to ask about any VS: "What evidence does it produce about the outcome, and why is it credible?"



1

A voting system must determine the winner *and* convince the losers they really lost.

- VS is not a "trusted party," but must justify its conclusions.
- VS must produce credible evidence that the stated outcome is correct.
- Key question to ask about any VS: "What evidence does it produce about the outcome, and why is it credible?"
- VS should include a (risk-limiting) audit to ensure that (with high probability) the evidence really does support the stated outcome.





 Different than banking or other information-processing applications.



- Different than banking or other information-processing applications.
- Voters should not be coerced or bribed (they must be protected from their own temptations).



- Different than banking or other information-processing applications.
- Voters should not be coerced or bribed (they must be protected from their own temptations).
- No one should know how a voter voted, even if the voter wants it. (Mandatory privacy!)



 Different than banking or other information-processing applications.

#2

- Voters should not be coerced or bribed (they must be protected from their own temptations).
- No one should know how a voter voted, even if the voter wants it. (Mandatory privacy!)
- Separation of voter identification from ballot makes good chain of custody very important.



 Different than banking or other information-processing applications.

#2

- Voters should not be coerced or bribed (they must be protected from their own temptations).
- No one should know how a voter voted, even if the voter wants it. (Mandatory privacy!)
- Separation of voter identification from ballot makes good *chain of custody* very important.
- VBM (vote-by-mail) and unsupervised remote voting are defective approaches.





Myth = We can build infallible machines that always work as specified.



- Myth = We can build infallible machines that always work as specified.
- Even when attacked!



- Myth = We can build infallible machines that always work as specified.
- Even when attacked!
- Ideal machine is equivalent to its specification.



- Myth = We can build infallible machines that always work as specified.
- Even when attacked!
- Ideal machine is equivalent to its specification.
- Real machine is what you get.



- Myth = We can build infallible machines that always work as specified.
- Even when attacked!
- Ideal machine is equivalent to its specification.
- Real machine is what you get.
- Rarely are these the same.

- Myth = We can build infallible machines that always work as specified.
- Even when attacked!
- Ideal machine is equivalent to its specification.
- Real machine is what you get.
- Rarely are these the same.
- Even good commercial software has several serious undiscovered errors per 1000 lines of code. These are frequently security vulnerabilities.



- Myth = We can build infallible machines that always work as specified.
- Even when attacked!
- Ideal machine is equivalent to its specification.
- Real machine is what you get.
- Rarely are these the same.
- Even good commercial software has several serious undiscovered errors per 1000 lines of code. These are frequently security vulnerabilities.
- Even worse, deployed implementation may have additional changes.



- Myth = We can build infallible machines that always work as specified.
- Even when attacked!
- Ideal machine is equivalent to its specification.
- Real machine is what you get.
- Rarely are these the same.
- Even good commercial software has several serious undiscovered errors per 1000 lines of code. These are frequently security vulnerabilities.
- Even worse, deployed implementation may have additional changes.
- Properties of system derive from properties of deployed system, not those of original spec.



#4 It may help to view a complex piece of technology as like a person.



#4 It may help to view a complex piece of technology as like a person.

 Automation / personification duality: Tasks once performed by people have been automated.



#4 It may help to view a complex piece of technology as like a person.

- Automation / personification duality: Tasks once performed by people have been automated.
- Just like a person, complex technologies can act in unpredictable, even malicious, ways. They can say one thing and do another.



#4 It may help to view a complex piece of technology as like a person.

- Automation / personification duality: Tasks once performed by people have been automated.
- Just like a person, complex technologies can act in unpredictable, even malicious, ways. They can say one thing and do another.
- Think of buying a voting system as you would hiring a team of workers from a temp agency.



4 It may help to view a complex piece of technology as like a person.

- Automation / personification duality: Tasks once performed by people have been automated.
- Just like a person, complex technologies can act in unpredictable, even malicious, ways. They can say one thing and do another.
- Think of buying a voting system as you would hiring a team of workers from a temp agency.
- Think of these workers as high-school students (earnest), elves (mischevious), or guys in ski masks (malicious).



4 It may help to view a complex piece of technology as like a person.

- Automation / personification duality: Tasks once performed by people have been automated.
- Just like a person, complex technologies can act in unpredictable, even malicious, ways. They can say one thing and do another.
- Think of buying a voting system as you would hiring a team of workers from a temp agency.
- Think of these workers as high-school students (earnest), elves (mischevious), or guys in ski masks (malicious).
- Imagine a voting machine, or the internet, as a "person." Did you ever make a hiring error?





An insider (election official or piece of technology) should not be able to undetectably corrupt evidence so as to cause change in outcome.



- An insider (election official or piece of technology) should not be able to undetectably corrupt evidence so as to cause change in outcome.
- Mental state of "temp worker" is at best weak or "hearsay" evidence.



- An insider (election official or piece of technology) should not be able to undetectably corrupt evidence so as to cause change in outcome.
- Mental state of "temp worker" is at best weak or "hearsay" evidence.
- Note difference between "job listing for the person you hired" and "the person who shows up for work on election day". For a machine, this is the difference between its specification and its actual behavior.



- An insider (election official or piece of technology) should not be able to undetectably corrupt evidence so as to cause change in outcome.
- Mental state of "temp worker" is at best weak or "hearsay" evidence.
- Note difference between "job listing for the person you hired" and "the person who shows up for work on election day". For a machine, this is the difference between its specification and its actual behavior.
- Misbehavior by an insider should be detectable (and correctable if possible!).



- An insider (election official or piece of technology) should not be able to undetectably corrupt evidence so as to cause change in outcome.
- Mental state of "temp worker" is at best weak or "hearsay" evidence.
- Note difference between "job listing for the person you hired" and "the person who shows up for work on election day". For a machine, this is the difference between its specification and its actual behavior.
- Misbehavior by an insider should be detectable (and correctable if possible!).
- Helps to distinguish "wholesale" from "retail" fraud.



- #6 Paper has cool properties!
 - Low-tech approach to constraining complex components, just as dog leash keeps dog from wandering off.



- Low-tech approach to constraining complex components, just as dog leash keeps dog from wandering off.
- Paper is human readable/writable, machine readable/writable, tamper-evident, and durable.



- Low-tech approach to constraining complex components, just as dog leash keeps dog from wandering off.
- Paper is human readable/writable, machine readable/writable, tamper-evident, and durable.
- A writing is a *commitment*-can't be easily changed.



- Low-tech approach to constraining complex components, just as dog leash keeps dog from wandering off.
- Paper is human readable/writable, machine readable/writable, tamper-evident, and durable.
- A writing is a *commitment*-can't be easily changed.
- VVPAT creates evidence—a set of facts—that can't be ignored or altered by VS. VS can't wander far from this set of facts.



- Low-tech approach to constraining complex components, just as dog leash keeps dog from wandering off.
- Paper is human readable/writable, machine readable/writable, tamper-evident, and durable.
- A writing is a *commitment*-can't be easily changed.
- VVPAT creates evidence—a set of facts—that can't be ignored or altered by VS. VS can't wander far from this set of facts.
- Audit is like yank on dog leash...





A voter *proxy* votes in your place.



- A voter *proxy* votes in your place.
- A voting *witness* watches you vote.



- A voter *proxy* votes in your place.
- A voting *witness* watches you vote.
- Proxy: You tell touch-screen voting machine (guy in ski mask) which candidate you prefer. Guy says he'll remember that and vote that way on your behalf later.



- A voter *proxy* votes in your place.
- A voting *witness* watches you vote.
- Proxy: You tell touch-screen voting machine (guy in ski mask) which candidate you prefer. Guy says he'll remember that and vote that way on your behalf later.
- Witness: You show scanner (elf) paper ballot you have filled out. Elf makes notes, and ballot goes into ballot box.



- A voter *proxy* votes in your place.
- A voting *witness* watches you vote.
- Proxy: You tell touch-screen voting machine (guy in ski mask) which candidate you prefer. Guy says he'll remember that and vote that way on your behalf later.
- Witness: You show scanner (elf) paper ballot you have filled out. Elf makes notes, and ballot goes into ballot box.
- In first case, guy is creating the evidence of your choices. In the second case, elf is merely observing the evidence you have created.



- #8 Avoid Internet Voting, for security reasons.
 - Why vote over the Internet? Why? Why?



- #8 Avoid Internet Voting, for security reasons.
 - Why vote over the Internet? Why? Why? Why?



- #8 Avoid Internet Voting, for security reasons.
 - Why vote over the Internet? Why? Why? Why? Why?



- #8 Avoid Internet Voting, for security reasons.
 - Why vote over the Internet? Why? Why? Why? Why? Why?...



Why vote over the Internet? Why? Why? Why? Why? Why?... Don't you have a better approach?



- Why vote over the Internet? Why? Why? Why? Why? Why?... Don't you have a better approach?
- Would you connect your toaster to a high-tension power line?



- Why vote over the Internet? Why? Why? Why? Why? Why?... Don't you have a better approach?
- Would you connect your toaster to a high-tension power line?
- Would you invest your pension in credit default swaps?

- Why vote over the Internet? Why?
 Why? Why? Why? Why?...
 Don't you have a better approach?
- Would you connect your toaster to a high-tension power line?
- Would you invest your pension in credit default swaps?
- Vendors who claim to have solved internet security problem are misleading you. (Like authors who write books on "How to make a million in real estate"—Why are they trying to make a buck writing how-to books?)



- Why vote over the Internet? Why? Why? Why? Why? Why?... Don't you have a better approach?
- Would you connect your toaster to a high-tension power line?
- Would you invest your pension in credit default swaps?
- Vendors who claim to have solved internet security problem are misleading you. (Like authors who write books on "How to make a million in real estate"—Why are they trying to make a buck writing how-to books?)
- Internet is useful in elections, but fails as an "channel of evidence for voter intent".





• Good for privacy and for *commitments*.



- Good for privacy and for *commitments*.
- With "end-to-end" (E2E) voting systems, voters cast encrypted ballots onto public "bulletin board."



- Good for privacy and for *commitments*.
- With "end-to-end" (E2E) voting systems, voters cast encrypted ballots onto public "bulletin board."
- Voters can verify encryption, without getting "receipt"(!).



- Good for privacy and for *commitments*.
- With "end-to-end" (E2E) voting systems, voters cast encrypted ballots onto public "bulletin board."
- Voters can verify encryption, without getting "receipt"(!).
- Bulletin board enables "verifiable chain of custody."



- Good for privacy and for *commitments*.
- With "end-to-end" (E2E) voting systems, voters cast encrypted ballots onto public "bulletin board."
- Voters can verify encryption, without getting "receipt"(!).
- Bulletin board enables "verifiable chain of custody."
- Authorities can produce tally without violating secret ballot.



- Good for privacy and for *commitments*.
- With "end-to-end" (E2E) voting systems, voters cast encrypted ballots onto public "bulletin board."
- Voters can verify encryption, without getting "receipt"(!).
- Bulletin board enables "verifiable chain of custody."
- Authorities can produce tally without violating secret ballot.
- Anyone can verify tally of encrypted ballots.



- Good for privacy and for *commitments*.
- With "end-to-end" (E2E) voting systems, voters cast encrypted ballots onto public "bulletin board."
- Voters can verify encryption, without getting "receipt"(!).
- Bulletin board enables "verifiable chain of custody."
- Authorities can produce tally without violating secret ballot.
- Anyone can verify tally of encrypted ballots.
- Scantegrity nicely integrates both paper ballots and crypto (for poll-site voting).



- Good for privacy and for *commitments*.
- With "end-to-end" (E2E) voting systems, voters cast encrypted ballots onto public "bulletin board."
- Voters can verify encryption, without getting "receipt"(!).
- Bulletin board enables "verifiable chain of custody."
- Authorities can produce tally without violating secret ballot.
- Anyone can verify tally of encrypted ballots.
- Scantegrity nicely integrates both paper ballots and crypto (for poll-site voting).
- Helios embodies similar ideas for remote voting (assuming that client is malware-free!).





You can't always get what you want:

non-fattening pizza



- non-fattening pizza
- totally safe cigarette



- non-fattening pizza
- totally safe cigarette
- getting fit with 5 minutes exercise/day



- non-fattening pizza
- totally safe cigarette
- getting fit with 5 minutes exercise/day
- automobile that runs on water



- non-fattening pizza
- totally safe cigarette
- getting fit with 5 minutes exercise/day
- automobile that runs on water
- secure internet voting (Calling something "secure" doesn't make it so. Maybe we should call this "wishful labeling". This happens a lot when marketing tells engineering what to invent.)



10 Voting system design is all about *tradeoffs*.



- #10 Voting system design is all about *tradeoffs*.
 - Security vs. Usability vs. Cost vs. Complexity vs. Accessibility vs. ...



#10 Voting system design is all about *tradeoffs*.

- Security vs. Usability vs. Cost vs. Complexity vs. Accessibility vs. ...
- Conflicting requirements drive up complexity.



#10 Voting system design is all about *tradeoffs*.

- Security vs. Usability vs. Cost vs. Complexity vs. Accessibility vs. ...
- Conflicting requirements drive up complexity.
- High complexity makes security tough.



10 Voting system design is all about *tradeoffs*.

- Security vs. Usability vs. Cost vs. Complexity vs. Accessibility vs. ...
- Conflicting requirements drive up complexity.
- High complexity makes security tough.
- Evidence-based elections may reduce need or cost for certification.



10 Voting system design is all about *tradeoffs*.

- Security vs. Usability vs. Cost vs. Complexity vs. Accessibility vs. ...
- Conflicting requirements drive up complexity.
- High complexity makes security tough.
- Evidence-based elections may reduce need or cost for certification.
- Continued research needed to identify interesting new design points, with different trade-offs. Need to understand first what voting systems are possible, then to select those that are "best".



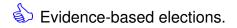
For more information

 Caltech/MIT Voting Technology Project.
 Voting: What Has Changed, What Hasn't & What Needs Improvement.
 October 2012.

http://vote.caltech.edu.

- Douglas W. Jones and Barbara Simons. Broken Ballots: Will Your Vote Count? CSLI, June 2012. http://brokenballots.com
- Verified Voting. http://verifiedvoting.org/
- Overseas Vote Foundation http://www.overseasvotefoundation.org
- Brennan Center for Justice http://www.brennancenter.org/









Evidence-based elections.

P Complex technology.





- Evidence-based elections.
- Complex technology.
- Paper is cool. Paper is prudent.





- Evidence-based elections.
 - Complex technology.
- Paper is cool. Paper is prudent.



Internet voting isn't ready for prime time.





- Sevidence-based elections.
 - Complex technology.
- Paper is cool. Paper is prudent.
- Internet voting isn't ready for prime time.
- Auditability.





- Sevidence-based elections.
 - Complex technology.



- Paper is cool. Paper is prudent.
- $\ref{eq:product}$ Internet voting isn't ready for prime time.

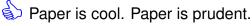


- Auditability.
- Post-election audits.





- Fvidence-based elections.
 - Complex technology.



 $\ref{eq:product}$ Internet voting isn't ready for prime time.



Auditability.



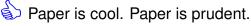
Post-election audits.

Cryptography and end-to-end voting.





- Evidence-based elections.
 - Complex technology.



Internet voting isn't ready for prime time.



Auditability.



- Post-election audits.
- Cryptography and end-to-end voting.
- Voting tech best of breed for poll-site voting seems to be:
 - Opscan ballots with post-election auditing.
 - End-to-end voting sytems.



Thank you!

!!! Please vote !!!

