Thoughts On Appropriate Technologies for Voting

Ronald L. Rivest

Viterbi Professor of EECS
MIT, Cambridge, MA

Princeton CITP E-voting Workshop
2012-11-01

Is Voting “Keeping Up with Technology”?

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

CSAIL

Is Voting “Keeping Up with Technology”?

- 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.

CSAIL

Is Voting “Keeping Up with Technology”?

- 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”?

CSAIL

Is Voting “Keeping Up with Technology”?

- 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”?
- Why are many of us voting on paper ballots?

CSAIL

Is Voting “Keeping Up with Technology”?

- 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”?
- Why are many of us voting on paper ballots?
- Why not voting, say, over the Internet?

CSAIL

Choosing Appropriate Technology for Voting

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

Choosing Appropriate Technology for Voting

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

CSAIL

Choosing Appropriate Technology for Voting

- 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.

CSAIL

Choosing Appropriate Technology for Voting

- 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)

CSAIL

Choosing Appropriate Technology for Voting

- 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.

CSAIL

Choosing Appropriate Technology for Voting

- 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?)

CSAIL

Choosing Appropriate Technology for Voting

- 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.

CSAIL

Epigrams

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?”

CSAIL

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.

CSAIL

2

The need for *secret ballots* makes voting system design both unique and hard.

2 The need for *secret ballots* makes voting system design both unique and hard.

- Different than banking or other information-processing applications.

2 The need for *secret ballots* makes voting system design both unique and hard.

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

2 The need for *secret ballots* makes voting system design both unique and hard.

- 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!)

2 The need for *secret ballots* makes voting system design both unique and hard.

- 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!)
- Separation of voter identification from ballot makes good *chain of custody* very important.

CSAIL

2 The need for *secret ballots* makes voting system design both unique and hard.

- 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!)
- Separation of voter identification from ballot makes good *chain of custody* very important.
- VBM (vote-by-mail) and unsupervised remote voting are defective approaches.

3 Beware of the “myth of the machine”!

3 Beware of the “myth of the machine”!

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

3 Beware of the “myth of the machine”!

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

3 Beware of the “myth of the machine”!

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

CSAIL

3 Beware of the “myth of the machine”!

- 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.

CSAIL

3 Beware of the “myth of the machine”!

- 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.

CSAIL

3 Beware of the “myth of the machine”!

- 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.

CSAIL

3 Beware of the “myth of the machine”!

- 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.

3 Beware of the “myth of the machine”!

- 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.

CSAIL

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.

CSAIL

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).

CSAIL

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?

CSAIL

5 VS must be robust against “insider attacks”!

5 VS must be robust against “insider attacks”!

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

5 VS must be robust against “insider attacks”!

- 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.

CSAIL

5 VS must be robust against “insider attacks”!

- 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.

CSAIL

5 VS must be robust against “insider attacks”!

- 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!).

5 VS must be robust against “insider attacks”!

- 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.

CSAIL

6 Paper has cool properties!

6 Paper has cool properties!

- Low-tech approach to constraining complex components, just as dog leash keeps dog from wandering off.

6 Paper has cool properties!

- 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.

CSAIL

6 Paper has cool properties!

- 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.

CSAIL

6 Paper has cool properties!

- 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.

CSAIL

6 Paper has cool properties!

- 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...

CSAIL

7

There is a difference between a *voter proxy* and a *voting witness*.

7 There is a difference between a *voter proxy* and a *voting witness*.

- A voter *proxy* votes in your place.

7 There is a difference between a *voter proxy* and a *voting witness*.

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

7 There is a difference between a *voter proxy* and a *voting witness*.

- 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.

7 There is a difference between a *voter proxy* and a *voting witness*.

- 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.

CSAIL

7 There is a difference between a *voter proxy* and a *voting witness*.

- 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.

CSAIL

8 Avoid Internet Voting, for security reasons.

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? Why?

8 Avoid Internet Voting, for security reasons.

- Why vote over the Internet? Why? Why? Why? Why? Why?...

8 Avoid Internet Voting, for security reasons.

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

8 Avoid Internet Voting, for security reasons.

- 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?

8 Avoid Internet Voting, for security reasons.

- 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?

8 Avoid Internet Voting, for security reasons.

- 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?)

8 Avoid Internet Voting, for security reasons.

- 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".

9 Cryptography can help.

9 Cryptography can help.

- Good for privacy and for *commitments*.

9 Cryptography can help.

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

9 Cryptography can help.

- 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”(!).

CSAIL

9 Cryptography can help.

- 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.”

CSAIL

9 Cryptography can help.

- 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.

CSAIL

9 Cryptography can help.

- 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.

CSAIL

9 Cryptography can help.

- 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).

CSAIL

9 Cryptography can help.

- 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*!).

10 Beware wishful thinking!

You can’t always get what you want:

10 Beware wishful thinking!

You can't always get what you want:

- non-fattening pizza

10 Beware wishful thinking!

You can't always get what you want:

- non-fattening pizza
- totally safe cigarette

10 Beware wishful thinking!

You can't always get what you want:

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

10 Beware wishful thinking!

You can't always get what you want:

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

CSAIL

10 Beware wishful thinking!

You can't always get what you want:

- 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.)

CSAIL

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.

CSAIL

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.

CSAIL

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.

CSAIL

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”.

CSAIL

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/`

Summary

Evidence-based elections.

Summary


Evidence-based elections.


Complex technology.

CSAIL

Summary


Evidence-based elections.


Complex technology.


Paper is cool. Paper is prudent.

CSAIL

Summary


Evidence-based elections.


Complex technology.


Paper is cool. Paper is prudent.


Internet voting isn't ready for prime time.

CSAIL

Summary


Evidence-based elections.


Complex technology.


Paper is cool. Paper is prudent.


Internet voting isn't ready for prime time.


Auditability.

CSAIL

Summary


Evidence-based elections.


Complex technology.


Paper is cool. Paper is prudent.


Internet voting isn't ready for prime time.


Auditability.


Post-election audits.

CSAIL

Summary


Evidence-based elections.


Complex technology.


Paper is cool. Paper is prudent.


Internet voting isn't ready for prime time.


Auditability.


Post-election audits.


Cryptography and end-to-end voting.

CSAIL

Summary

 Evidence-based elections.

 Complex technology.

 Paper is cool. Paper is prudent.

 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.

CSAIL

Thank you!

!!! Please *vote* !!!