# Internet Voting–Seriously??

Ronald L. Rivest

Institute Professor
MIT, Cambridge, MA

EVN Conference
2016-03-11

# Outline

Introduction

Technology evolution and voting

Internet voting

Security

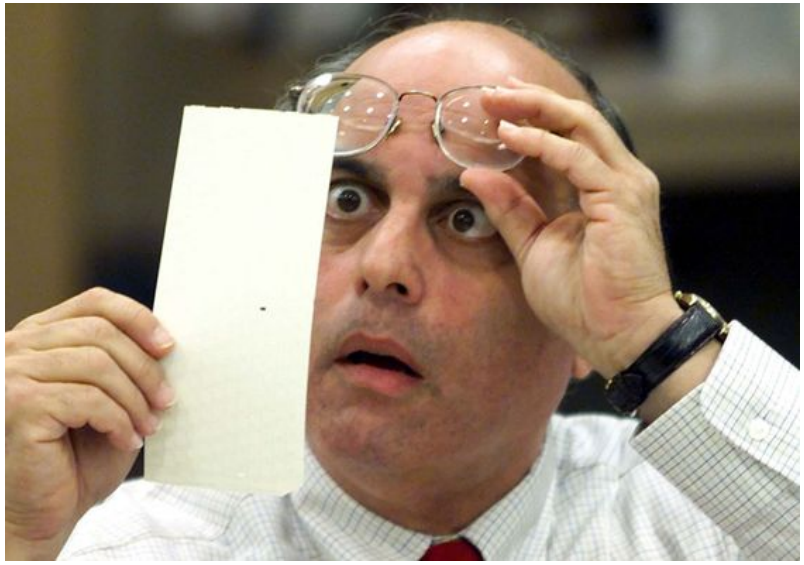
Risk assessment

# New tech for old applications

One often asks if new technology can improve existing applications...

# New tech for old applications

One often asks if new technology can improve existing applications...
Example: punch cards for voting

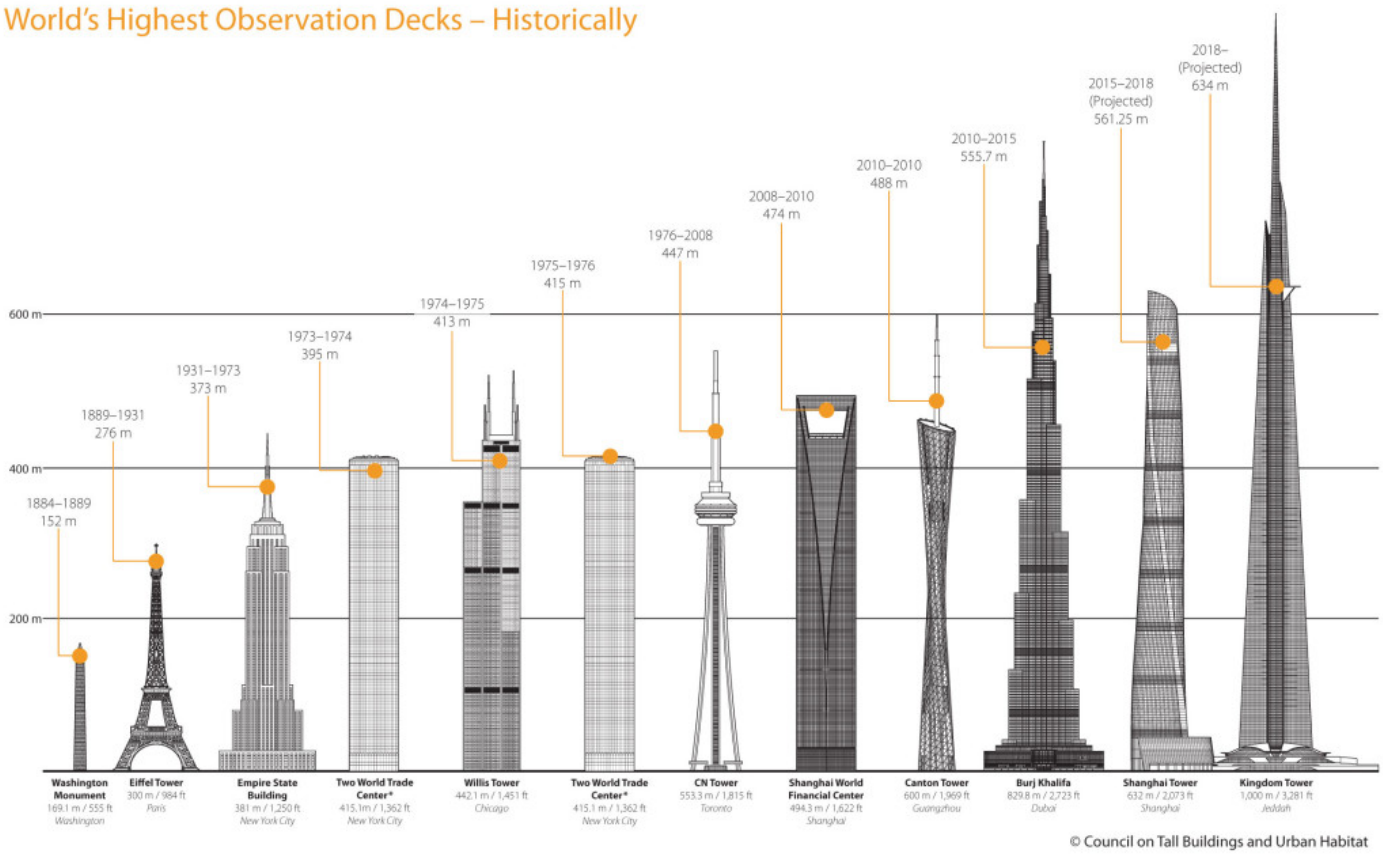


Step forward... or a mistake?

CSAIL

# Sometimes new tech helps

# Sometimes new tech helps




Electric motors → elevators → tall buildings.

CSAIL

# Sometimes it doesn’t, or is silly.

# Sometimes it doesn't, or is silly.

CSAIL

# Sometimes it is too dangerous for some uses!

# Sometimes it is too dangerous for some uses!

(Don’t text while driving!)

CSAIL

# Can using the Internet help elections & voting?

Yes, in many ways it can be helpful:

- Distributing information about an election and choices.

# Can using the Internet help elections & voting?

Yes, in many ways it can be helpful:

- Distributing information about an election and choices.
- Allowing voters to update their personal information.

CSAIL

# Can using the Internet help elections & voting?

Yes, in many ways it can be helpful:

- Distributing information about an election and choices.
- Allowing voters to update their personal information.
- Providing information about election results.

CSAIL

# Can using the Internet help elections & voting?

Yes, in many ways it can be helpful:

- Distributing information about an election and choices.
- Allowing voters to update their personal information.
- Providing information about election results.
- Providing information about audit of election results...

CSAIL

# Can using the Internet help elections & voting?

Yes, in many ways it can be helpful:

- Distributing information about an election and choices.
- Allowing voters to update their personal information.
- Providing information about election results.
- Providing information about audit of election results...
- ...

CSAIL

# Can using the Internet help elections & voting?

Yes, in many ways it can be helpful:

- Distributing information about an election and choices.
- Allowing voters to update their personal information.
- Providing information about election results.
- Providing information about audit of election results...
- ...

CSAIL

# Can using the Internet help elections & voting?

Yes, in many ways it can be helpful:

- Distributing information about an election and choices.
- Allowing voters to update their personal information.
- Providing information about election results.
- Providing information about audit of election results...
- ...

But... actually voting over the Internet????

CSAIL

# What is “Internet Voting (IV)”?

Internet voting is a form of remote voting.
Remote voting has many flavors:

- Ballots sent to voter by: mail | web | email
- Ballots are: paper | electronic | both
- Voters are: supervised | unsupervised
- Ballot “marked” by: voter | kiosk | voter PC
- Ballots returned by: mail | web | email
- Auditing: none | moderate | comprehensive

CSAIL

# What is “Internet Voting (IV)”?

Internet voting is a form of remote voting.

Internet voting:

- Ballots sent to voter by: mail | web | email
- Ballots are: paper | electronic | both
- Voters are: supervised | unsupervised
- Ballot “marked” by: voter | kiosk | voter PC
- Ballots returned by: mail | web | email
- Auditing: none | moderate | comprehensive

CSAIL

# IV Proponents suggest IV would help:

# IV Proponents suggest IV would help:

- High-tech “buzz”?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”?
- Extend franchise to military & disabled?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”?
- Extend franchise to military & disabled?
- Turnout?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”?
- Extend franchise to military & disabled?
- Turnout?
- Cost?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”?
- Extend franchise to military & disabled?
- Turnout?
- Cost?
- Security?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”? A+
- Extend franchise to military & disabled?
- Turnout?
- Cost?
- Security?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”? A+
- Extend franchise to military & disabled? B
- Turnout?
- Cost?
- Security?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”? A+
- Extend franchise to military & disabled? B
- Turnout? C
- Cost?
- Security?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”? A+
- Extend franchise to military & disabled? B
- Turnout? C
- Cost? D
- Security?

CSAIL

# IV Proponents suggest IV would help:

- High-tech “buzz”? A+
- Extend franchise to military & disabled? B
- Turnout? C
- Cost? D
- Security? F

CSAIL

# Voting must work in an *adversarial* environment

- **Q:** If we can put a man on the moon, why can't we make online voting work?

CSAIL

# Voting must work in an *adversarial* environment

- **Q:** If we can put a man on the moon, why can't we make online voting work?
- **A:** Because voting must work in an *adversarial* environment. You wouldn't get a man on the moon if people were trying to sabotage the launch and shooting at the rocket.

CSAIL

# Voting must work in an *adversarial* environment

- **Q:** If we can put a man on the moon, why can't we make online voting work?
- **A:** Because voting must work in an *adversarial* environment. You wouldn't get a man on the moon if people were trying to sabotage the launch and shooting at the rocket.
- **Note:** Adversaries may be outsiders, or insiders. A foreign nation-state is a *likely adversary*.

CSAIL

# Voting must provide a *secret ballot*

- **Q**: If we can bank online, why can't we make online voting work?

CSAIL

# Voting must provide a *secret ballot*

- **Q**: If we can bank online, why can't we make online voting work?
- **A**: Banking is not anonymous, so you can have identifiable receipts. Furthermore you can "undo" a bad banking transaction. Finally, bankers spend *lots* of money on security.

CSAIL

# Online voting security is an *unsolved problem*

- **Q**: Do we know how, even in theory, to make online voting secure?

# Online voting security is an *unsolved problem*

- **Q**: Do we know how, even in theory, to make online voting secure?
- **A**: **No.** Not even close.

CSAIL

# Online voting security is an *unsolved problem*

- **Q**: Do we know how, even in theory, to make online voting secure?
- **A**: **No.** Not even close.

CSAIL

# Online voting security is an *unsolved problem*

- **Q**: Do we know how, even in theory, to make online voting secure?
- **A**: **No.** Not even close.
  NIST: “additional research and development is needed to overcome these challenges before secure Internet voting will be feasible.” (No timeframe provided. No existing standards for IV.)
- NIST is being diplomatic. Secure Internet voting may in fact be an *unsolvable* problem.

# Some may say “Adversary won’t attack”

# The Internet is a war zone. Casualties are mounting.

- Easy challenge: Pick a random month within the last couple of years. Find a major company that was seriously hacked that month, which is bigger than all of the voting system vendors put together.

# The Internet is a war zone. Casualties are mounting.

- Easy challenge: Pick a random month within the last couple of years. Find a major company that was seriously hacked that month, which is bigger than all of the voting system vendors put together.
- Home Depot ($83B revenues in 2015) was hacked in 2014, disclosing 56 million credit card numbers. This week they agreed to pay $19M in fines; they expect to lose as much as $160M via lawsuits.

# Attackers are getting stronger and winning.

- “Advanced Persistent Threats”—Adversary keeps working on a company until it finds a “way in” to its systems.

CSAIL

# Attackers are getting stronger and winning.

- “Advanced Persistent Threats”—Adversary keeps working on a company until it finds a “way in” to its systems.
- Almost always succeeds, eventually.

CSAIL

# Attackers are getting stronger and winning.

- “Advanced Persistent Threats”—Adversary keeps working on a company until it finds a “way in” to its systems.
- Almost always succeeds, eventually.
- Recently Juniper Systems ($4B revenue 2014) found its source code had been hacked by unknown parties, leaving a “backdoor”.

CSAIL

# Attackers are getting stronger and winning.

- “Advanced Persistent Threats”—Adversary keeps working on a company until it finds a “way in” to its systems.
- Almost always succeeds, eventually.
- Recently Juniper Systems ($4B revenue 2014) found its source code had been hacked by unknown parties, leaving a “backdoor”.
- It may be months or years (average around 18 months) before a company even realizes it has been hacked.

# Sea change in security world assumptions

- The standard assumption used to be:

# Sea change in security world assumptions

- The standard assumption used to be:

  *With good design and careful implementation, you can prevent security problems.*

CSAIL

# Sea change in security world assumptions

- The standard assumption used to be:

  *With good design and careful implementation, you can prevent security problems.*

- Now the standard working assumption is more realistic/pessimistic:

CSAIL

# Sea change in security world assumptions

- The standard assumption used to be:

  *With good design and careful implementation, you can prevent security problems.*

- Now the standard working assumption is more realistic/pessimistic:

  *If you are online, you will be hacked (or already have been). "Assume the breach." Can you deal with it? Or even detect it?*

CSAIL

# Defenders are very weak in this space.

- Voting system vendors don't even show up at major security conferences! (Last week RSA Conference had 40,000 attendees and 500 vendors...)

CSAIL

# Defenders are very weak in this space.

- Voting system vendors don't even show up at major security conferences! (Last week RSA Conference had 40,000 attendees and 500 vendors...)
- I don't even know any cryptographers that work at a voting system vendor!

CSAIL

# Defenders are very weak in this space.

- Voting system vendors don't even show up at major security conferences! (Last week RSA Conference had 40,000 attendees and 500 vendors...)
- I don't even know any cryptographers that work at a voting system vendor!
- Security budgets for most election jurisdictions are miniscule.

CSAIL

# Internet voting is “proxy voting”.

- With proxy voting, a voter asks a proxy (person or perhaps a machine) to vote for her, following voter’s requested choices.

# Internet voting is “proxy voting”.

- With proxy voting, a voter asks a proxy (person or perhaps a machine) to vote for her, following voter’s requested choices.
- Several countries use proxy voting, a proxy (person) can vote for at most a small number (e.g. 4) of voters.

CSAIL

# Internet voting is “proxy voting”.

- With proxy voting, a voter asks a proxy (person or perhaps a machine) to vote for her, following voter’s requested choices.
- Several countries use proxy voting, a proxy (person) can vote for at most a small number (e.g. 4) of voters.
- With IV, you are asking a machine or online server to be your “proxy voter” and vote for you.

CSAIL

# Internet voting is “proxy voting”.

- With proxy voting, a voter asks a proxy (person or perhaps a machine) to vote for her, following voter’s requested choices.
- Several countries use proxy voting, a proxy (person) can vote for at most a small number (e.g. 4) of voters.
- With IV, you are asking a machine or online server to be your “proxy voter” and vote for you.
- If one machine proxies for millions of voters, you have a large risk if proxy is hacked. (And as we saw, we should assume that server has been hacked!)

# Remote voting already has known security problems

- Unsupervised remote voting vulnerable to vote-selling, bribery, and coercion.

CSAIL

# Internet voting has additional security problems

- Malware (both server and client).

CSAIL

# Internet voting has additional security problems

- Malware (both server and client).
- Network may be unreliable/manipulable. DOS attacks can selectively kill voting in selected jurisdictions.

CSAIL

# Internet voting has additional security problems

- Malware (both server and client).
- Network may be unreliable/manipulable. DOS attacks can selectively kill voting in selected jurisdictions.
- Strong voter authentication methods lacking.

CSAIL

# Internet voting has additional security problems

- Malware (both server and client).
- Network may be unreliable/manipulable. DOS attacks can selectively kill voting in selected jurisdictions.
- Strong voter authentication methods lacking.
- Every software system has yet-to-be discovered vulnerabilities (“0-days”).

CSAIL

# Internet voting has additional security problems

- Malware (both server and client).
- Network may be unreliable/manipulable. DOS attacks can selectively kill voting in selected jurisdictions.
- Strong voter authentication methods lacking.
- Every software system has yet-to-be discovered vulnerabilities (“0-days”).
- Attacks can be automated, executed on a massive scale, and done so anonymously. Including automated vote-buying schemes.

# Internet voting has additional security problems

- Malware (both server and client).
- Network may be unreliable/manipulable. DOS attacks can selectively kill voting in selected jurisdictions.
- Strong voter authentication methods lacking.
- Every software system has yet-to-be discovered vulnerabilities (“0-days”).
- Attacks can be automated, executed on a massive scale, and done so anonymously. Including automated vote-buying schemes.
- ...

# Auditable elections

- An election system must produce not only the *correct outcome*, but also an auditable *evidence trail* sufficient to convince even the most skeptical loser that she lost fair and square.

CSAIL

# Auditable elections

- An election system must produce not only the *correct outcome*, but also an auditable *evidence trail* sufficient to convince even the most skeptical loser that she lost fair and square.
- The audit should be "*software independent*" and *not* assume that the election system software has behaved correctly. (It may have been hacked.)

CSAIL

# Auditable elections

- An election system must produce not only the *correct outcome*, but also an auditable *evidence trail* sufficient to convince even the most skeptical loser that she lost fair and square.
- The audit should be "*software independent*" and *not* assume that the election system software has behaved correctly. (It may have been hacked.)
- Paper ballots and "end-to-end verifiable audit logs" are two useful evidence-producing methods.

CSAIL

# Can we make IV secure?

- We do not currently have the technology to make internet voting secure (and may never).

CSAIL

# Can we make IV secure?

- We do not currently have the technology to make internet voting secure (and may never).
- We can't make such technology appear by wishful thinking, just trying hard, making analogies with other fields, or running pilots.

CSAIL

# Can we make IV secure?

- We do not currently have the technology to make internet voting secure (and may never).
- We can't make such technology appear by wishful thinking, just trying hard, making analogies with other fields, or running pilots.
- It is irresponsible to assume that determined effort by an adversary won't defeat IV security.

CSAIL

# Helios

- Best internet voting system I know: “Helios” by Ben Adida (former PhD student of mine).

CSAIL

# Helios

- Best internet voting system I know: “Helios” by Ben Adida (former PhD student of mine).
- Ben says firmly, “A government election is something you don’t want to do over the Internet.”

CSAIL

# Technology abuse

- Some folks are just be a bit too infatuated with the latest tech...

CSAIL

# Technology abuse

- Some folks are just be a bit too infatuated with the latest tech...
- They ask,

  “What are best practices for internet voting?”

CSAIL

# What is the best way to play in traffic?

# What is the best way to play in traffic?

CSAIL

# What is the best way to become roadkill?

# What is the best way to become roadkill?

CSAIL

# Internet Voting Summary

CSAIL

# Internet Voting Summary

*Wargames (1983)*:

CSAIL

# Internet Voting Summary

*Wargames (1983)*:

"Sometimes the only winning move is

# Internet Voting Summary

*Wargames (1983)*:

"Sometimes the only winning move is *not to play*."

CSAIL

# We don’t need to play in traffic!

(Footbridge = paper ballots)

CSAIL

# Moving forward...

- Many people seem to want to “vote on the Internet” (why?????)

# Moving forward...

- Many people seem to want to “vote on the Internet” (why?????)
- Most don’t recognize the severe security problems it entails

# Moving forward...

- Many people seem to want to “vote on the Internet” (why?????)
- Most don’t recognize the severe security problems it entails
- More research is reasonable (e.g. could a blockchain help??),

CSAIL

# Moving forward...

- Many people seem to want to “vote on the Internet” (why?????)
- Most don’t recognize the severe security problems it entails
- More research is reasonable (e.g. could a blockchain help??),
- But one shouldn’t expect near-term (10-year) “solutions”

CSAIL

# Moving forward...

- Many people seem to want to “vote on the Internet” (why?????)
- Most don’t recognize the severe security problems it entails
- More research is reasonable (e.g. could a blockchain help??),
- But one shouldn’t expect near-term (10-year) “solutions”
- Indeed, this isn’t the kind of problem that has a “solution” preventing security breaches; one rather needs good procedures for dealing with the certainty of getting hacked and dealing with DOS attacks.

# The End

# What about “end-to-end” internet voting?

An “end-to-end” voting system provides additional auditing capabilities for voters and others to detect when the election has “gone awry.”

Without paper ballots, an E2E voting system doesn’t provide much in the way of a recovery mechanism to determine and restore the correct election outcome once a problem is detected.

Nonetheless, the recent U.S. Vote Foundation report on internet voting recommends that E2E voting properties are *necessary* (but not sufficient) for internet voting systems.

CSAIL