Thoughts on UOCAVA Voting

Ronald L. Rivest

Viterbi Professor of EECS
MIT, Cambridge, MA

UOCAVA Workshop
2010-08-06

C S A I L

Outline

C S A I L
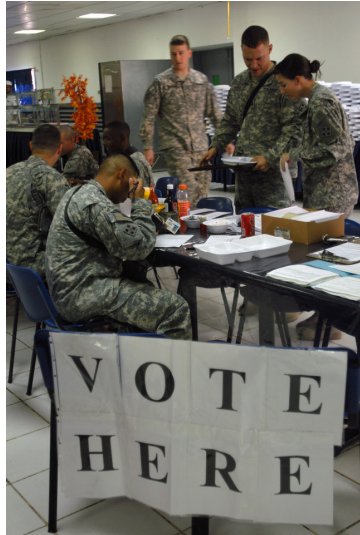
UOCAVA voters

How should soldiers and overseas citizens best exercise their right to vote?

Remote voting

Remote voting has many flavors:

- ▶ Ballots sent to voter by: mail | internet
- ▶ Ballots are: paper | electronic | both
- ▶ Voters are: supervised | unsupervised
- ▶ Ballot "marked" by: voter | kiosk | voter PC
- ▶ Ballots returned by: mail | internet | both
- ▶ Auditing: none | moderate | comprehensive

C S A I L

Remote voting

Remote voting has many flavors:

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

"Internet voting"

CSAIL

Remote voting

Remote voting has many flavors:

- ▶ Ballots sent to voter by: mail | internet
- ▶ Ballots are: paper | electronic | both
- ▶ Voters are: supervised | unsupervised
- ▶ Ballot "marked" by: voter | kiosk | voter PC
- ▶ Ballots returned by: mail | internet | both
- ▶ Auditing: none | moderate | comprehensive

My recommendation

CSAIL

Short summary of this talk:

- ► Remote voting is trade-off between franchise and risk.

Short summary of this talk:

- Remote voting is trade-off between franchise and risk.
- The risks of "internet voting" more than negate any possible benefits from an increase in franchise.

C S A I L

Short summary of this talk:

- Remote voting is trade-off between franchise and risk.
- The risks of "internet voting" more than negate any possible benefits from an increase in franchise.
- We should give UOCAVA voters the best possible paper ballot system we can manage!

C S A I L

Evaluation criteria for remote voting systems

- Availability and usability
- Cost
- Staffing requirements
- Security and auditability

Evaluation criteria for remote voting systems

- Availability and usability
- Cost
- Staffing requirements
- Security and auditability

C S A I L

Remote voting already has known security problems

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

- Communication with voter, and transmission of ballots, may be unreliable/manipulable.
- I believe remote voting should be allowed:
  - only as needed
  - for at most 5% of voters
- UOCAVA voting meets these criteria.

CSAIL

Internet voting has additional security problems

- Platform insecurity (both client and server)
- Network insecurity
- Set of attackers enlarged from:
  - just those who can touch paper ballots, to
  - anyone on the planet with a computer
- Attacks can be automated, executed on a massive scale, and done so anonymously

CSAIL

Platform insecurity (both client and server)

- Modern computer systems only provide modest security — they are puzzle boxes rather than vaults.
- Once adversary solves the puzzle, he can open it (and all others like it).

Internet voting

We may view internet voting as voting on a contraption consisting of a collection of such puzzle boxes, all connected by untraceable wires to every possible adversary on the planet.

C S A I L

Internet voting

We may view internet voting as voting on a contraption consisting of a collection of such puzzle boxes, all connected by untraceable wires to every possible adversary on the planet.
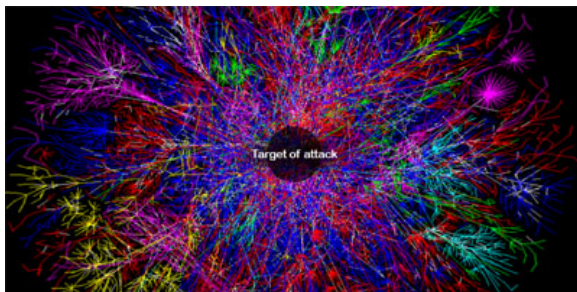

CSAIL

Network insecurity

Most serious problem may be DDOS attack, which can make remote internet voting system simply unavailable to UOCAVA voters.

C S A I L

Risk Assessment of internet voting

Let's just look at most serious risk:
adversarial attack changes the election outcome

C S A I L

Let's just look at most serious risk:
adversarial attack changes the election outcome
— a *failure of democracy*.

C S A I L

Net benefit

= benefit – loss

CSAIL

Net benefit – a proposed metric

Net benefit

= benefit – loss

= % new voters given franchise
  –
  % voters losing franchise through fraud

CSAIL

Net benefit – a proposed metric

Net benefit

= benefit – loss

= % new voters given franchise
–
% voters losing franchise through fraud

(We'll use *expected values* here, although you can't justify using probabilities on adversarial actions!)

CSAIL

Benefit

What is plausible *benefit*? (Worked example)

- ▶ Suppose UOCAVA voters are 2% of registered eligible voters.
- ▶ Suppose that new technology enables increase in franchise by 1% .
  (E.g. suppose increase from 0.5% to 1.5%)
  (I consider this an optimistic estimate!)
- ▶ We'll estimate (potential) benefit as 1%.

CSAIL

Loss

Can we estimate % voters we expect to lose franchise through fraud?

Loss

Can we estimate % voters we expect to lose
franchise through fraud?

Fact:

If adversary determines election outcome,
all voters are disenfranchised!

We no longer have a democracy in action...

C S A I L

Hall of Shame Factor

- What is "loss" when election is stolen? Just the 100% loss of franchise?

- Let's add an additional Hall of Shame Factor (HOSF), for stolen elections. (Not only shame, but if elections are (or could be) stolen, voters may get cynical and not vote again!)

C S A I L

Loss

- Suppose we let HOSF = 4
  (something between 1 and 10)
- Then loss for a stolen election is
  $100\% * \text{HOSF} = 400\%$.

Expected loss
- = expected % voters disenfranchised by fraud
- = Prob(Adv steals election)
  - $* 100\% * \text{HOSF}$
- = $400\% * \text{Prob(Adv steals election)}$

C S A I L

Prob(Adv steals election)

Prob(Adv steals election) =
Prob(election is close enough) $*$
Prob(Adv attacks voting system) $*$
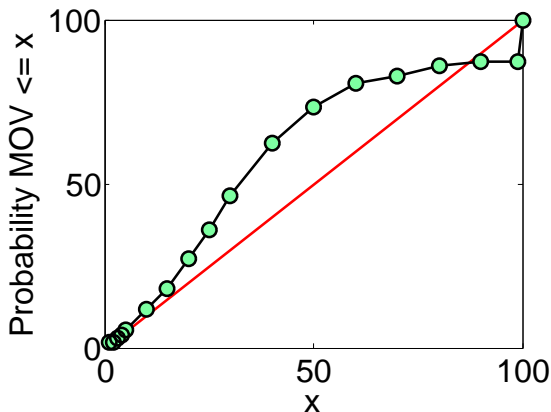Prob(attack succeeds)

How often are elections "close"?

- **Def:** The *margin of victory* (MOV) is (winner's share) - (loser's share) as % .

How often are elections "close"?

- **Def:** The *margin of victory* (MOV) is (winner's share) - (loser's share) as % .
- Empirically Prob(MOV $\leq$ x%) = x%.
- 2008 Congressional election data:

CSAIL

How often are elections "close enough" for fraud?

- Suppose UOCAVA votes are 1.5% of total.
- If security were truly terrible, and Adv controlled all cast UOCAVA votes, then Adv could steal election 1.5% of the time (when MOV $\leq$ 1.5%), by casting all UOCAVA votes for his candidate, who would otherwise lose.
- So, in this example,
  Prob(election is close enough) = 1.5%

CSAIL

Will Adversary attack voting system?

- Is the Pope Catholic?
- Will someone pick up $20 left on sidewalk?
- There is nothing to deter attacker – Adv can attack anonymously over the Internet until he succeeds.
- Do you know of any computer systems that have never been attacked?
- Prob(Adv will attack voting system) = 100%

C S A I L

Some may say "Adversary won't attack"

Will Adv succeed in attack?

- ▶ Would you even know?
- ▶ If there are no audits, no one will be the wiser, and he can continue successful attack method in each election.
- ▶ Days are past for IIB election management. (IIB = Ignorance Is Bliss) (Also known as WIDKWHM policy.)

CSAIL

Will Adv succeed in attack?

- ► Large institutions (banks, Google) are successfully attacked all the time. They have much better staff and budgets!

- ► Bob Morris (NSA) said: "You will always underestimate the effort the enemy will make to break your system."
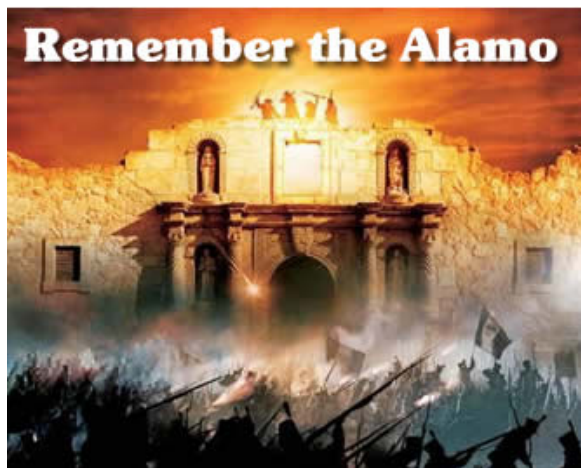
A bigger attack than you expected!

Superior force wins the day!

Who has more IT capability – your local election
IT staff or the Chinese?

Superior force wins the day!

Who has more IT capability – your local election IT staff or the Chinese?

Remember the Alamo

(They lost.)

Will Adv succeed in attack?

- 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 imprudent (irresponsible?) to assume that determined effort by adversaries can't defeat security objectives of internet voting.

C S A I L

Will Adv succeed in attack?

- 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 imprudent (irresponsible?) to assume that determined effort by adversaries can't defeat security objectives of internet voting.

Prob(Adv succeeds) = 100%

C S A I L

Expected loss

Expected loss

=	$400\% * \text{Prob(Adv steals election)}$
=	$400\% * \text{Prob (election close)}$
	$* \text{Prob(Adv attacks)}$
	$* \text{Prob(attack succeeds)}$
=	$400\% * 1.5\% * 100\% * 100\%$
=	6%

CSAIL

What's the net benefit or loss?

Net benefit
    = 1% gain
       –
      6% loss
    = - 5% net loss

One step forward, six steps backward.

CSAIL

Risk Assessment Conclusion

- Based on this risk assessment, we expect Internet voting for UOCAVA voters to disenfranchise many more voters than it would franchise.

- The apparent gains in franchise for internet voting are misleading and illusory—the apparent gains are more than cancelled by the risks.

- Argument is robust — conclusion remains the same even if numbers are varied significantly. In addition, there may be a DDOS attack with probability near 100%.

CSAIL

Helios

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

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."

Summary

Summary

Internet voting

Summary

Internet voting
is like

CSAIL

Internet voting
is like
drunk driving

Internet voting
is like
drunk driving

(Just too risky!)

CSAIL

Technology abuse

- Some folks may have had just a bit too much to drink at the "technology bar"...
  (Technology can be intoxicating!)

Technology abuse

- ► Some folks may have had just a bit too much to drink at the "technology bar"...
  (Technology can be intoxicating!)
- ► "What are best practices for internet voting?"

CSAIL

Technology abuse

- ► Some folks may have had just a bit too much to drink at the"technology bar"...
  (Technology can be intoxicating!)

- ► "What are best practices for internet voting?" to me sounds like
  "Pleash jush help me inshert the key in the lock, (hic), and I'll be on my way..."

CSAIL

- Some folks may have had just a bit too much to drink at the "technology bar"...
  (Technology can be intoxicating!)

- "What are best practices for internet voting?" to me sounds like
  "Pleash jush help me inshert the key in the lock, (hic), and I'll be on my way..."

- The goal should be responsible use of technology!

C S A I L

Technology abuse

- Some folks may have had just a bit too much to drink at the"technology bar"...
  (Technology can be intoxicating!)

- "What are best practices for internet voting?" to me sounds like
  "Pleash jush help me inshert the key in the lock, (hic), and I'll be on my way..."

- The goal should be responsible use of technology!

- Friends don't let friends drive drunk!

C S A I L

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.

CSAIL