Internet Voting
Possibilities and Perils

Jonathan A. Goler
MIT/Caltech Voting Technology Project
MIT Media Lab
Internet Voting Outline

✓ Part 1: Historical Voting/Security Practices
✓ Break
✓ Part 2: Perils.
✓ Break
✓ Part 3: Solutions, Techniques and Practices
Historical Voting Practices

✓ Significant differences in voting performance due to race, socio-economic status and disabilities.
✓ Non-Electronic processes lead to significant and sometimes systematic disenfranchisement.
A Brief History

✓ Greece: Stones
✓ Early US: Limited suffrage & non-secret ballots
✓ Edison: Electronic Voting Machine
✓ Lever Machines
✓ Punchcards
✓ Direct Recording Electric (DRE)
Technology is not the only problem

- Cook county card undercount variation .75 % to 39%, non random!
- Paper 1.8%
- Punch Card 2.5
- Optical Scan 1.5
- Lever Machine 1.5
- DRE 2.3

- States rely on many different technologies.
- Sometimes, technology is deployed differentially.
Many Sources of Lost Votes

Confusing ballot 1 - 2 million
*Incumbent top on ballot?*

Polling place operations 1 million
*Intermediaries improve confidence?*

Absentee ballots ??
*Rampant coercion?*

Stolen or changed?
*People make mistakes*

Registration 1 - 3 million +
*Registration is obsolete?*

Nov 2000 Votes

The process has to want the votes

5/21/04
Current Registration Practice

✓ Non-coordinated registrars
✓ HAVA “drive thru” registrations with DMV
  ✓ No Registration
  ✓ Paper Rolls
  ✓ Databases
  ✓ Some ID required, some ID prohibited
✓ No Checks!

5/21/04
Problems have not been voter verifiable

- Brevard 4000 Back end software
- Volusia 16022 Back end software
- Boone County 10000 Back end software
- Washington State Altered paper ballots
- Dallas Destroyed paper ballots
- Many places Replaced paper ballots
- Georgia Not close enough to recount
- Indiana (?) User interface (Straight vote)
- Recent Republican Shown on UI
- Mail in Absentee No secrecy
Coercion?

- We disagree so let's neither vote
  - 15 years later one spouse had been voting all along
- Ballot marking parties at churches
- We like this guy
  - Said a 45 year old child to their parent in a voting booth
- Nursing homes
  - They have a right to vote
- Palm cards
- Precinct Captain
- Ballot layout
- Order on Ballot
- Stand in voters

  • Humiliation,
  • Intimidation,
  • Hand over hand voting
  • Misinformation
  • Parallax and other physical access
    — (arm extension)
Reference Platform: Brazil

Renewed belief in government!!

- **Electronic voting; 96, 98, 2000**
  - 96 Unisys 7% failure
  - 98 Procomp
  - 2000 Procomp .02% failure 106,000,000 votes

- **Trusted Scientific organization**
  - Create requirements

- **Trusted Technical organization**
  - Create reference platform

- **Companies (5)**
  - Create demonstratable products for bid

- **Government election officials**
  - Create open viewing and decision of vendor

5/21/04
Technologies to improve voting

✓ Electronic Security
  ✓ SAVE: N-Version Architectures
  ✓ Closed systems: (game machines with CD)

✓ Ballot Design
  ✓ Orienting design with feedback
  ✓ Knowledge based tool for improving ballot design

✓ Verification
  ✓ Frog
  ✓ Audio Verification
  ✓ Analysis of VVPT

✓ Registration
  ✓ Open information XML registration checker
What Needs To Be Done

✓ Future of fraud prevention:
  ✓ Policies
  ✓ Practices
  ✓ Architectures

✓ Polling places outdated?
✓ Voting information is changing
✓ New voting approaches are being explored
  ✓ Cell phone, Interactive TV, Kiosk, extended hours, vote by mail
  ✓ Same day registration
  ✓ Instant runoff
  ✓ Compulsory voting
  ✓ Direct democracy
"Bad ballot design gave highest error rates"
Perceptual

✓ Graphical
  ✓ View ability, Color, contrast, size,
  ✓ Readability, Distinctions, Distinguishably
  ✓ Precognitive, cognitive,
  ✓ Feedback; Proprioceptive,

Cognitive Interface

✓ Precognitive recognition issues, Recognition VS Recall (except when conflicting)
✓ Short term memory 7 +- 2 (in 2 d), depth of info 2 or three
✓ Cognitive load, syntactic, semantic. bored ... overloaded

Social issues

✓ You are doing Great...
✓ Your Vote Matters
✓ Androgynous Voice...

Cognitive Styles

✓ Verbal/ Visual
✓ Procedural/Conceptual
✓ Myers Briggs
✓ Physical, perceptual, psychological, neurological
Software Testing Questions

- When to worry about what problems
  - Current processes uninformed and uneven
    - Code build to change ballot?
    - Bugs found/ fixed within weeks of elections?
    - Machine rooms open, ...

- Trust LEO chosen experts on software?
  - Don’t know any
  - Don’t take them seriously

- Do code reads really help
  - Hidden code?

- Does sharing product code with public help
  - Encourage hacking?
Severe Lack of Technical Oversight

- Some election companies have one technologist...
- Time on voting machines can be changed
- Standard Socketed EPROM's, cables without seals, ...
- Reboot problems,
- Connectors effect vote
- Practice or real election?
- Training voters on live machines (Broward 2003)
- Optical scan
  - Alignment problems normal
  - Jamming normal
  - Security of ballots:
    - Hands in box, exchange, storage, disposal, defacing
Will openness help short term – vs.- long term

- Diebold not alone in problematic programming practices
  - US Voting technology marketing driven
  - Economics of voting technology
  - Security Experts in demand elsewhere
- Election officials self taught
- Election companies are obvious consultants on elections
- Experts, peer review, (building and running)
Historical Questions

 ✓ What Historical precedents in Voting are important to keep and which should we change?

 ✓ How important is secrecy of the ballot? It was not always secret.

 ✓ How can we learn from fraud patterns in the past to perhaps yield improved detection?
Physical Security

✓ Machines now are not generally physically secure.
✓ Warehouses store thousands of voting machines
✓ Pre-Election testing is unable to find bugs/security breaches if hardware is compromised

5/21/04
User Interfaces

✓ Currently: Horrible
✓ However, they prevent things like overvoting
✓ Feedback timing
  ✓ Currently often not immediate
  ✓ Many voters ignore feedback
Disenfranchisement

- Large Text Ballots (low vision)
- Assisting in filling out (nursing homes)
- Physical disabilities
Internet Voting Perils
Internet Voting Perils

✓ Security of the Ballot
✓ Secrecy of the Ballot
✓ Coercion of voters
✓ Denial of Service
✓ Potential for large scale, undetected fraud
✓ => Loss of Confidence in System
Ballot Security Issues

✓ Pre-submitted ballot
✓ Uncontrolled environment
✓ Uncontrolled equipment
Mistakes and fraud

Protection, detection & correction

- Observation, Confidentiality, Redundancy
- Universal verifiability
  - Voter verifiable results verifiability
- COTS good or bad?
Secrecy of the Ballot

✓ If a ballot is on a remote machine, with no security, who makes sure that people do not know how a user voted?

✓ Internal threats: software/viruses

✓ External threats: tempest
Coercion Issues
Systemic Vote Buying

- Door to door grassroots vote buying
- Internet based vote buying
- Spouse/parent influence
- More nefarious influence (blackmail, intimidation)
Denial of Service (Voters)

✓ Individual machines can be targeted
  ✓ Virus: mac only... mac owners more likely to be democrats...
  ✓ Inexperienced users could not deal with a DOS attack
  ✓ Experienced users may not be able to recover in time.
  ✓ Proof of disruption to computer
Denial of Service (Servers)

✓ Voting collection/administration machines could be attacked
  ✓ DOS attack prevents and frustrates voters
  ✓ Undermines confidence in system
Consequences

✓ Electronic voting equipment is already getting a bad rep
  ✓ Diebold
✓ Administrators jumping into new technology too quickly, resulting in a backlash.
The BIG Problem:

Large scale, undetectable fraud.
So what do we do?
What to do...

✓ Apply Technology, practice, and oversight
✓ Provide Voter Verification as a fallback, and as a confidence building measure
✓ Use the advantages of electronic voting such as fast tabulation, and usability improvements
✓ Use security techniques EFFECTIVELY
✓ Move slow enough to get it right

5/21/04
Technology and practices
Each useful in different situations

- Technology
  - Encryption, Public key, N-version, hardened systems...

- Practices
  - Secrecy
    - Military, Security industry, governments, banks,...
  - Oversight
    - Expert review
    - Redundancy
    - Open source
Verification goal = Air-Gapping

Alternatives:
Votemeter, modular architecture, encrypted votes, open source, process, standards, VVPT

- VVPT: insecure
- Audio: available now
- Video: available now
- Votematic: needs development
- N-Version: needs development
Software problems have been routed in process

✓ Brevard 4000       Back end software
✓ Volusia 16022      Back end software
✓ Boone County 10000  Back end software
✓ Washington State   Altered paper ballots
✓ Dallas              Destroyed paper ballots
✓ Many places         replaced paper ballots
✓ Georgia             Not close enough to recount
✓ Indiana             User interface (Straight vote)
✓ Recent Republican   shown on UI
✓ Mail in Absentee    No secrecy
Voter Verification
Many experts, particularly outspoken are Rebecca Mercuri, David Dill and Avi Rubin, claim that Voter Verifiable Paper Trails (VVPTs) are the only means of ensuring that a vote is cast and counted properly.

A VVPT is a receipt produced by a DRE that records the votes in human readable and tangible form.
The “Buzz” on VVPT

✓ Many experts claim that Voter Verifiable Paper Trails (VVPTs) are the only means of ensuring that a vote is cast and counted properly
✓ Laziness aside (Chicago), VVPTs are confusing.
  ✓ Delayed feedback is too late to do something about failures
  ✓ Having to compare two potentially different looking documents is confusing
✓ Printers are prone to failure
✓ Fraud still possible

5/21/04
Problems with a separate paper trail.

- No way for ballot worker to help
- Connection broken
- Paper out
- Paper Jam
- Ink out
- Printer broken
- Paper looks different
- Different format than DRE
- Separate thing to look at

- Extra time & step for voting
- Lighting, readability
- Special needs (Dyslexia, ADHD, blind )
- Extra steps for ballot worker
- Collecting the ballots
- Ballots could be exchanged
- Re-voting a machine at end of day
- Rereading ballots
Hacking a VVPT

- Hack vote and print almost readable receipt 1 in 50
- 1 in 10 people that see that do anything (Chicago)
- 1 in 500 (one per precinct sees this problem)
  - Print again - it fixes itself
  - Call a judge - first time in the day at that polling place
    - They say print it again - it fixes itself
    - They come into the booth - yikes they are arrested!
    - They shut down the booth - yikes only a few machines
An Audio Audit trail
with today’s DRE hardware

- Stored on a tape and spoken from it (built in integrity)
- Speaks each selection (perceptual not memory task)
- Advantages
  - machine verifiable,
  - improves user interface,
  - voting box integrity, storability, transportability
Camera Audit Trail
Can be done now

- Camera or video cable record screen as you do it.
- You see the feed on a non computer screen
- Record on a tape or CD
- Advantages to VVPT
  - Ballot box integrity, verify as you go, machine readable
Votemeter audit trail
System would have to be built

- Separate machine with code from others
- Shows same ballot selections as made
- Records them separately
- Advantages
  - Machine readable
  - Ballot box integrity
  - Usability
N-version audit trail

- Voter UI Client Software
  - Bitmap is the only shared thing in system
- Voter Authentication Software
  - Multiple competing authentication systems must agree
- Voter Aggregating Software
  - Multiple competing aggregating systems must agree
- Vote verification Software
  - While anonymous voter can view vote, later that it is there
Secure Architecture for Voting Electronically

No single anything voting

UI, registration, witness and aggregator layers…

Voter can authenticate datum while voting.

Voter and voter system See the same bitmap

Votes live on multiple viewable databases

Votes live on a viewable databases
Internet Voting Techniques
Two Forms of Internet Voting

1. True Vote from Home voting
2. Schoolhouse/precinct voting
Salient Advantages of IV

✓ Expanded opportunity for enfranchisement
  ✓ More flexibility than precinct voting
  ✓ More languages

✓ More specific adaptations for disabilities:
  ✓ Reading Disabled, Low Vision
  ✓ Tactile Interfaces, Audio Interfaces
User Interface Questions

✓ What UI improvements can help
  ✓ Level the playing field for candidates (drop off)
  ✓ Reduce undervoting
  ✓ Reduce disparities associated with socioeconomic status
1. Each eligible voter shall be allowed to vote at most once.

2. Every vote cast must be counted accurately.

3. No vote cast must be traceable back to an individual.
Cryptographic Security

✓ Public and Symmetric Key cryptography.
  ✓ PKI: Smartcards for everyone?
  ✓ AES? Not for our purposes

✓ Signatures
  ✓ FIPS 186-2 Secure Digital Signatures
  ✓ Secure Hashes (MD5, SHA-1)

✓ Blind Signatures

✓ Homomorphic Encryption

5/21/04
Public Key Cryptosystems

✓ RSA Standard:
  ✓ Good key length 2048 bits
  ✓ Not proven to be secure, but it has withstood scrutiny, with no known cracks (relies on the difficulty of factoring primes)
  ✓ Slow
  ✓ Depends on Public Key Infrastructure (PKI)
Advanced Encryption Standard.

New, intense scrutiny, symmetric block cipher.

Key material is symmetric so it is not a good idea to put that in voting equipment.
PKI & Smartcards

✓ Smartcards are credit card sized devices that contain a chip that contains a private signing key.
✓ All computation is performed ON the card, so you do not give out your key to other hardware
✓ Power analysis lets you read off the key in real time. (VERY BAD)
Blind Signatures

✓ Fujuoka, Okamota, Ohta Blind Signature Scheme
✓ Take a message, and a piece of carbon paper
✓ Put them into an envelope
✓ Sign the outside of the envelope
✓ Put the envelope in a bin
✓ Remove the envelope and the signature is on the message inside.
Crypto Weaknesses

✓ Key Length, while commonly considered vital, tends to be an easy problem to deal with
✓ Cipher mode: ECB/CBC VITAL
✓ Key Material: Good randomness
✓ Key security (physical security vital)
Coercion Solutions
Coercion is a huge problem for internet voting.

Can’t have a person in every house ensuring no coercion.

Solutions: Allow internet voting from monitored/public locations (schools, libraries).
Coercion - Fundamental Problem

✓ Coercion is a fundamental problem with mail-in balloting anyways, so we can not do worse.
✓ Solution impossible without differential information (which must be distributed to the voter directly, in person)
Digital Signatures

✓ Take a plaintext message
✓ Hash it (using a secure hash algorithm such as SHA-1)
✓ Encrypt the plaintext using private key
✓ Verification: decrypt signature and compare to hash of message.
✓ Message cannot change without disrupting the hash of the message and the signature is secure.
Chaum Method

- Specialized Printers
- Use a bitmap of ballot, encoded text.
- 2 sheets: keep one, it proves nothing (cryptographically), but can be used to verify vote in the final tally.
- Voter has a verifiable receipt that does not prove how she/he voted.

5/21/04
Frog Method

✓ Tangible votes
✓ “Frog” because the medium is not important
  ✓ Discs
  ✓ Paper
  ✓ Smartcards
✓ People can see, feel, touch it.

5/21/04
The SAVE Voting System

N-version programming + crypto
A Proposal for a Better System

✓ The SAVE (Secure Architecture for Voting Electronically) Architecture
✓ No Single point of failure voting (except the voter of course)
The SAVE Architecture

✓ N-version programming: do not trust any one company/group/person.

✓ Cryptographic protocols:
  ✓ Blind Signatures
  ✓ Public Key encryption
  ✓ Mix-Nets (secure shuffle)
Voting

✓ 2 possibilities: @ home, @ precincts
✓ And 2 variants: PC / Playstation
✓ @ precincts is easier to secure
✓ @ home presents inherent problems of the untrusted myriad environments possible.
✓ System implemented could be either PC or “Playstation” model.

5/21/04
PC Model

✓ Software must be loaded on the PC (presently it would be the JRE, keys and the user interface)
✓ Steps must be taken to ensure that nothing on the computer can see what the user is doing (this is hard)
Playstation Model

✓ Send out CDs that can be loaded into a playstation, now we can run without a real OS
✓ Perhaps we could do this for PCs?
✓ This approach is better for security, less likelihood for monitoring, but it could still be done.
✓ Introduces the problem of writing drivers for modems and other devices.
User Interface

✓ FEEDBACK!!!!!!!!!!!

✓ Visualize the State of the Ballot:
  ✓ What has been done (including choices)
  ✓ What has to be done

✓ Confirm Abstentions

✓ Review Ballot before Submitting
Tabs Indicate Selections

Please make your selection for President

Click on a candidate's name to select them, or click on a selected candidate to de-select them. Your selection will be indented and darkened.

- AL GORE
- GEORGE W BUSH
- RALPH NADER
- No Choice
- Write In
Please make your selection for President
Click on a candidate's name to select them,
or click on a selected candidate to de-select them.
Your selection will be indented and darkened.

AL Gore [Selected]
George W. Bush
Ralph Nader
No Choice
Write In

I'm Finished
Please make your selection for US Senator
Click on a candidate’s name to select them,
or click on a selected candidate to de-select them.
Your selection will be indented and darkened:

- Edward Kennedy
- Jackie Robinson
- Loony Independent
- No Choice[SELECTED]
- Write In

I'm Finished
✓ Aggregator servers’ public keys and sent off along with the registration data to the registration server.

✓ Registration database must be kept on an accessible server, which can be queried from the outside.

✓ The Registration Servers should never receive a plaintext vote. Blind Signatures are the best solution.
Validation - Witnesses

✓ We allow for “witness” modules, that can be in the form of smartcards(preferable) or merely additional modules.

✓ Witnesses receive a hash of the ballot and produce a time stamped(to ensure uniqueness) digital signature for that ballot.
Aggregation

✓ Decrypt the outer ballot package.
✓ Verify the signatures of the registration server, as well as the witness signers.
✓ Decrypt the inner ballot package, which actually contains the plaintext ballot.
✓ Randomly verify hashes of the incoming ballots with other servers, but do a full verification afterwards.
Ballot Designer

✓ Automatic and Manual Rule-Based Layout
✓ Enforces legal requirements
✓ Ensure uniformity
✓ Account for cognitive differential correction.
✓ Standard language (BDL-XML) IEEE 1622
Conclusions

✓ Internet voting, in some form, is coming.
✓ Steps need to be taken to make sure that the first generation is done right
✓ Oversight, standards, and rigorous review are necessary to inspire trustworthiness
Our Recommendations

✓ Prohibit remote (home) internet voting
✓ Promote schoolhouse voting with an internet infrastructure
  ✓ Redundancy
  ✓ End to end security
  ✓ UI advantages

5/21/04
Requiring Standards

✓ IEEE 1583 Voting Equipment Standard
✓ IEEE 1622 Voting Data Interchange Standard
✓ Incorporate data security standards as they improve or are proved insufficient
  ✓ FIPS 186-2,3
  ✓ ANSI X9
  ✓ IETF
✓ FIPS Key management standard under development
A “Friendly” Warning

We get one chance in a generation, or we will be back to optical scan
Acknowledgements

✓ MIT Caltech Voting Technology Project
  ✓ Carnegie Foundation
✓ Professor Ted Selker
✓ Professor Steve Ansolabehere