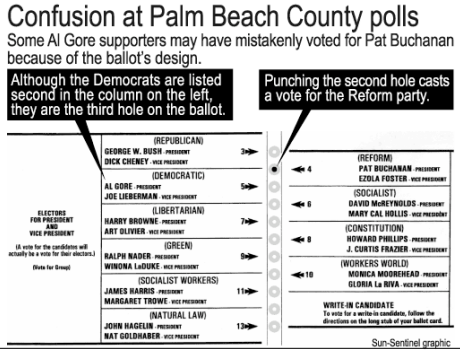
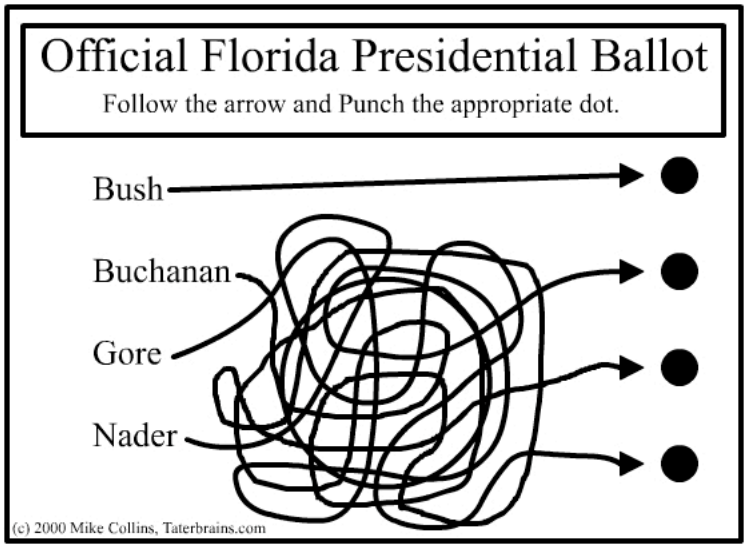
Security considerations for e-voting

Motivation

- National election debacle
  - Outcry for improved process





Technology

- Technology improves
  - Travel
  - Transportation
  - Accounting
  - Entertainment
  - Communications

Natural question:

Why not use it to improve elections?

1997 Costa Rican Election

- My first experience with e-voting…

Costa Rica

- In Costa Rica
  - Election is like a national holiday
  - People are required to vote
  - Voting is in home precinct
  - People do not update precinct when they move
  - Government pays for people to travel home
  - Special government tribunal is in charge of elections.

Costa Rica

- Approached my colleague, Lorrie Cranor
  - She enlisted our security group
  - Together with lawyers from Villanova
- Goal: to use computers from the schools
  - Bring them to polling sites
  - Network them together
  - Verify registration at *any* polling site
- Wanted to run trial at several polling sites in upcoming election

Costa Rica - challenges

- Ballet was different for each voter depending on where they lived (local elections)
- Large number of people not computer literate
  - Could not grasp concept of a *mouse* in studies
- New equipment, touch screens, light pen, etc. cost money that they did not have
- US crypto export policy at the time
  - We could not develop a system in the US and bring it there
- Would voters trust a US developed system?

Decisions

- Limit registration to polling places
  - Voters only have to trust local poll workers, not crypto programmers from the US
- Use light pens (touch screens too expensive)
  - Our employer would foot the bill for the trial
- Use a hardened O/S with only voting functionality
- Run trial in parallel with real election

Outcome

- Several weeks of design and brainstorming by our security group
  - Came up with a reasonable design
- Trip to Costa Rica by me, Lorrie and the Villanova lawyers
  - All day meeting with election tribunal
    - Seemed to go well
- In the end they got cold feet
  - Afraid that loser would dispute the election outcome because of our trial
- Trial was cancelled

Lessons learned in Costa Rican project

- Elections have much different security requirements than any other system
  - Outcome is almost guaranteed to be challenged
  - Public confidence in the security of the system is at least as important as the actual security
  - Access must be equal regardless of computer experience, age, and disabilities
  - The threat model is different
    - Foreign governments, major companies, marquis hackers
    - "Flag day" for attack
  - Denial of service can undermine the whole thing

Other lessons learned

There is nothing that can bring a group of security researchers together like the chance to influence the outcome of the election in another country.

A free trip to Costa Rica is an opportunity not to be missed.

Florida

- Press from Costa Rica project:
  - Led to Florida election officials visiting the Labs in 1997
  - Interested in electronic elections for the state
  - Wide-scale corruption caused funds to be allocated away from this project

"They could have been using our system in Florida in 2000!"

-- someone in our group

NSF e-voting workshop

- next experience with e-voting

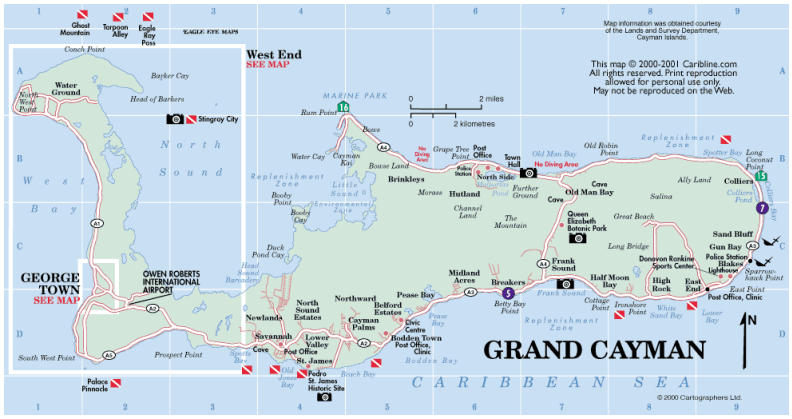
NSF Workshop October, 2000

- By request of President Clinton
- Chaired by C. D. Mote Jr., President of the University of Maryland
- Brought together technologists, social scientists, state and national election officials, dept. of justice, and the NSF
- Former US senator in attendance
- 2 days of discussion about e-voting from every possible angle
- Several sessions on security

NSF Report

- Workshop led to widely circulated report
  - Sent to White House and Congress
- Key Recommendations
  - We are ill prepared for remote e-voting
  - There is hope for electronic poll sites

Financial Cryptography



- Next experience with e-voting

Financial Cryptography

- Panel: The Business of Electronic Voting
- February, 2001 in Grand Cayman
- Chair: Moti Yung, CertCo
- Panelists: Ed Gerck, safevote.com
  Andy Neff, VoteHere.net
  Ron Rivest, MIT
  Avi Rubin, AT&T Labs

The Business of Electronic Voting

- Safevote:
  - Some wild claims: solved DDOS, solved platform issues.
- Votehere:
  - Offered a more balanced perspective, pleaded with the research community for help, some novel crypto techniques
- Technical panelists
  - Listed challenges, overall skeptical about Internet voting, cautiously hopeful about poll site voting
- Audience
  - Passionate discussion, personal attack against a panelist

Panel demonstrated that emotions run high when it comes to elections and threats to democracy

Conference on Internet & Democracy

- Swedish consulate in NYC, Mar. 29-30, '01
- I talked about e-voting security
- Audience
  - Mostly non-technical, lawyers, social scientists
  - Shocked by my opinions, highly doubted me
  - Asked me if it was so risky, how come more computer scientists are not complaining

Consulate General of Sweden
New York

2001 USENIX Annual Technical CONFERENCE

June 25–30, 2001
Marriott Copley Place Hotel
Boston, Massachusetts

- Boston, June 29, 2001
- Gave an invited talk on security issues for remote electronic voting

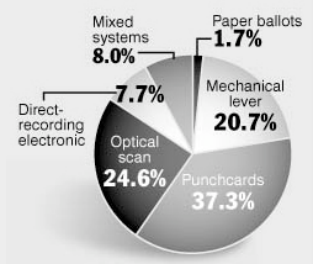


Voting machines

Types of voting machines

Type of voting system	How the system works	Advantages	Disadvantages
Paper ballots	Voters mark choices on ballots and drop them in a sealed box.	Inexpensive; used mostly in rural areas.	Counting votes is slow and labor-intensive.
Mechanical lever	Voters pull a lever assigned to a candidate.	Easy to use; prevents multiple votes for the same race.	Machines can weigh 900 pounds and are no longer manufactured.
Punchcards	Voters punch holes in a ballot; ballots are then read by a computer.	Cheaper; more portable.	Can be inaccurate and unreliable; hand recounts pose problems.
Optical scan	Voters darken an oval or rectangle next to their choice; ballots are then read by a computer.	Easy to use; the process is similar to marking lottery tickets or standardized tests; hand recounts are possible.	Improperly marked ballots may not be recorded; high cost.
Direct-recording electronic	Touch-screen electronic display.	Easy to use; vote totals can be instantly printed on tape and recorded on a cartridge.	Computers provide no external way to verify vote accuracy.

1996 Presidential election:



Poll site voting

- Computerized voting machines
  - Automatic counting
  - GUI display with pictures possible
  - Perhaps network linkage across sites
  - Leading candidate:
    - Direct Recording Electronic (DRE) machines
      - Vote counted in a cartridge
      - Already being deployed in many places

The poll site of the future…

- Allow partial votes and revised votes
- Fail-safe electronic balloting (ha ha)
- Integration of registration databases and ballot selection systems
- Ballots in multiple languages or layouts
- Real-time reporting of who has voted
- Real-time tallies
- Screen size, ballot format, navigability
- On-screen electioneering

Desirable properties of voting machines

- Voter feels that
  - Vote was counted
  - Vote was private
  - Nobody else can vote more than once
  - Nobody can alter others' votes
- People believe that the machine works correctly and that its behavior cannot be modified
- These have to do with *perception*.

It is also important that these perceptions are true.

Audit trail

- It is important that all phases of the vote casting and counting be auditable
- Recounts must be possible
  - If results come into question
- For electronic systems, need to audit
  - Hardware and software development
  - System deployment
  - All system binaries (compiled code, as well as compiler)
  - Use of system

Currently, such audit of hardware and software is not common, and is considered very difficult, if not impossible.

Electronic systems

- Several well understood concepts
  - The more software, the more flaws
  - Electronic systems are expected to fail at times
  - We talk about *failure modes*, not whether or not things fail
- Software security
  - It is very difficult to examine software and understand its behavior
    - Especially with malicious programmer
  - It is difficult to know that a particular source code matches a particular binary
  - It is difficult to know that a particular binary is installed on a particular platform
- There are many anecdotes of voting systems failing…

Voting System failures (from newspapers)

- “In Middlesex County, NJ, in 2000, a DRE vote-counting computer recorded votes for both the Republican and Democratic candidates in the county freeholder’s race, but accidentally wiped out all votes for their respective running mates.”

- “In the 1985 Dallas, TX, mayor’s race, Starke Taylor defeated Max Goldblatt in an election so controversial that it led the Texas legislature to investigate the flaws in the state’s computerized vote-tabulation process. Allegedly, according to the Dallas Morning News, a computer had been shut off and given "new instructions" after it showed Goldblatt leading by 400 votes.

  This case prompted the Texas Secretary of State to direct that, in future elections, a "manual recount" could be ordered to "ensure the accuracy of the count." The actual ballots, the computer punch cards themselves, are the only existing "audit trail," to document how people actually voted.”

More stories

- During the Democratic presidential primary of 1980, in Orange County, CA, a "programmer’s error" gave about 15,000 votes cast for Jimmy Carter and Ted Kennedy to Jerry Brown–and, Lyndon LaRouche.
- Computers in Oklahoma skipped 10 percent of the ballots in a 1986 election.
- A power surge in San Francisco switched votes from one candidate to another.
- A Moline, IL, city alderman actually took office in 1985 only to step down three months later when someone figured out that a machine had misread hundreds of ballots due to a bad "timing belt."

An example e-voting system

Sensus

- Created by Lorrie Craner and based on Fujioka, Okamoto, Ohta (FOO)
- Participants
  - Voter
  - Voter agent (totally trusted component, runs locally)
  - validator - ensure one vote per person
  - tallier - count ballots and report results

Not designed for Internet voting in public elections.

Blind signatures

- Need validator to sign m
- Validator should not know value of m
- Voter must be able to verify blind signature
- Assume RSA scheme
  - $n = pq$, where p and q are large primes
- Analogy of envelope with carbon paper in it
- Public exponent of validator is e, signing exponent is d

Blind Signatures (Chaum)

- All arithmetic is mod n
- Blinding (performed by voter):
  - choose a random blinding factor r
  - compute and present for signing: $m \times r^e$ where m is the message
- Signing (performed by validator):
  - compute $(m \times r^e)^d$
  - this is equal to $r \times m^d$
- Unblinding (performed by voter):
  - compute $r \times m^d / r = m^d$

Validator

- Public key pair: *ve*, *vd*
- Registered Voter List (RVL)
  - voter IDs
  - voter public keys
  - whether voter ballot has been validated (dynamically updated)

se, sd	ballot seal key
ie, id	voter key pair
ve, vd	validator key pair
te, td	talier key pair
K	blinding factor

Tallier

- public key pair: *te*, *td*
- ve (validators public key)
- T: election tally
- Receipt List (RL)
  - list of receipts sent out
  - corresponding sealed ballots
  - decyption keys
  - recipt numbers

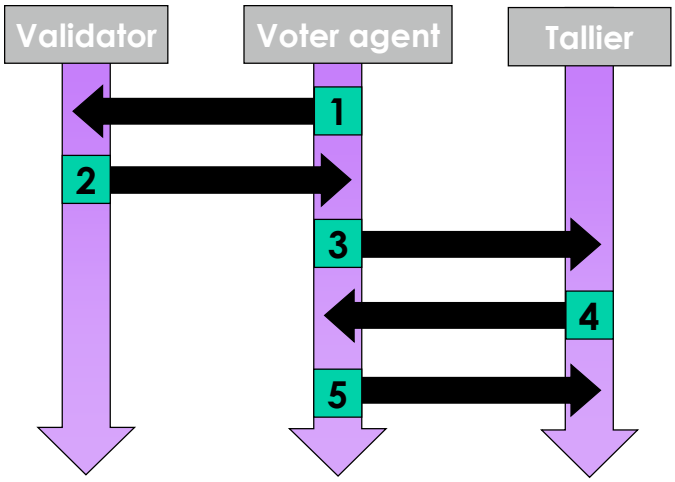
se, sd	ballot seal key
ie, id	voter key pair
ve, vd	validator key pair
te, td	talier key pair
K	blinding factor

Voter agent

- V: a voted ballot
- ID, voter ID number
- ballot seal key pair: *se*, *sd*
- $m = V^{se}$ (sealed vote)
- k = large random number for blinding
- voter key pair: *ie*, *id*
- talliers and validator public keys: *te*, *ve*
- $b = m\ k^{ve}$ (blinded, sealed ballot)

se, sd	ballot seal key
ie, id	voter key pair
ve, vd	validator key pair
te, td	talier key pair
K	blinding factor

The Sensus Polling Protocol



The Sensus protocol

- Voter agent sends validator, sealed with *ve*
  - *b*: blinded, sealed ballot
  - ID: ID number
  - b^{id}: *b*, signed with *id*, voter private key
- Validator unseals with *vd* and
  - verifies that $b = (b^{id})^{ie}$, checks the signature on *b*
  - updates RVL (registered voters list)
  - signs *b*
  - sends b^{vd} to voter agent, after sealing with *ie*
- Net result is that validator signs *b*

se, sd	ballot seal key
ie, id	voter key pair
ve, vd	validator key pair
te, td	talier key pair
K	blinding factor

Sensus (cont.)

- Voter agent unseals with *id*
  - unblinds b^{vd} by dividing by *k*
  - obtains m^{vd} which is *m*, signed by validator
  - verifies that $(m^{vd})^{ve} = m$
  - sends (m^{vd}, V^{se}) to tallier, sealed with *te*
- tallier unseals with *td* and
  - verifies: $V^{se} = (m^{vd})^{ve}$
  - signs V^{se} to produce $(V^{se})^{td}$ = receipt
  - updates RL with a receipt # and sealed ballot
  - sends $(V^{se})^{td}$, receipt # to voter agent

se, sd	ballot seal key
ie, id	voter key pair
ve, vd	validator key pair
te, td	talier key pair
K	blinding factor

Sensus (cont.)

- Voter agent verifies receipt

  checks that $V^{se} = ((V^{se})^{td})^{te}$

  sends ballot secret key, *sd*, and receipt number to tallier
- tallier

  opens V^{se} with *sd*

  updates RL and T

se, sd	ballot seal key
ie, id	voter key pair
ve, vd	validator key pair
te, td	talier key pair
K	blinding factor

Evaluation of Sensus

- Accuracy
  - altered, eliminated, and invalid votes can be detected and corrected
- Democracy
  - if voters abstain, validator may submit ballots for them
  - these invalid ballots may be detected, but not corrected
- Privacy
  - not possible to link a ballot to the voter who cast it
  - does not prevent a voter from proving how he or she voted
    - Could potentially solve with last-vote-counts process
- Verifiability
  - voters can verify that their ballots were counted correctly and protest anonymously

Why inadequate for Internet voting

- Assumes communication occurs over an anonymous channel
- Machines (along with secrets on them) are secure
  - No Trojans, viruses, worms
  - Trusted O/S, applications, bug-free platform
- Assumes no subliminal channels in RSA
  - Depends on the implementation (no random padding)
- Assumes network is highly available
- Assumes there is a national registry of identities and public keys.
  - Assumption: election PKI is available in all places where it is adopted

Material goods vs. Democracy

- Rich people have lots of money, poor people do not
- You can buy, sell, trade material goods
- You can always gain or lose money
- If economy falters, many people lose money

- Everybody has one vote
- You are not supposed to barter your vote
- You will always have just one vote
- If democracy falters everybody loses freedom

Public elections are not like other transactions.

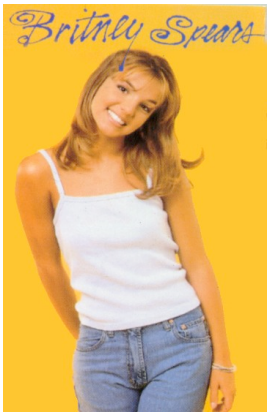
Some thoughts on e-voting:

Threats

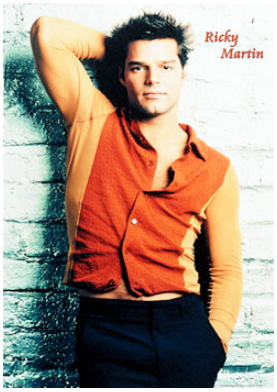
- Gauge the threat. Based on:
  - Type of election (public vs. private)
  - Consequences of a successful attack
  - Value of election outcome to potential adversaries
  - Expertise, skill & resources needed to disrupt
  - Level of motivation of potential attackers
  - Amount of disruption needed to sway the election or call its outcome into doubt
  - Consequences of a perception of unfair outcome

Low threat election

- Vote for your favorite pop artist:



Brittney Spears



Ricky Martin


Destiny's Child

Higher threat election

- Vote for the leaders of the free world
  - Affects military spending
  - Taxes
  - Relationship with other countries
  - Crime
  - Education
  - How to spend a VERY large budget

Internet voting in public elections

NOT!

- Social issues:
  - Vote coercion
  - Vote sale
  - Vote solicitation (*click here to vote*, banner ads)
- Technical issues:
  - Securing the platform
  - Securing the communications channel
  - Assuring availability of the network
  - Registration issues, one vote per person, no dead voters
  - Authentication in each direction
  - Maintaining equitable costs (no poll tax, e.g. smartcard reader)

Platform issues

- The following can influence PC behavior (Wintel environment)
  - Hardware manufacturer, O/S vendor, all applications (MS office, quicken, browser, anti-virus software), any downloaded software (e.g. screen savers), any visitor with physical access, any virus (e.g. Love bug, Melissa)
  - Remote control software: PC Anywhere, Backorifice.
  - Exploitation of bugs
- Would these be used to subvert an election?

  It depends on the threat model, the importance of the election, and the resources of the adversary.

Communications channel

- We know how to secure a channel (crypto)
  However, it is only as secure as the endpoints
- technical solutions exist for:
  - Verifiable elections, privacy preserving, accurate, convenient, efficient, last-vote wins, etc.
- BUT, 2 missing assumptions:
  - Adversary has control of voter's computer
  - Adversary can deny service to any subset of voters

Assuring network availability

- The Internet is vulnerable to denial of service attack
  - Syn floods, smurf attacks, ping of death (one packet to crash a computer)
  - The way we deal with this is to detect and punish (hard to prevent)
  - DDOS raises the stakes even higher
  - Attacks have been demonstrated in practice
- In a public election, could bring down portions of the Net, e.g. by demographic

A teenager in Canada (mafia boy) made national headlines (Feb, 2000), what could a government with billions of dollars do?

The Importance of Diversity

- In biological systems
  - Gene diversity ensures that a virus or a disease cannot wipe out an entire population
- In computer systems
  - Platform diversity (operating system, browser version) ensures that a computer virus does not infect every system
- In voting systems
  - Diversity limits the damage that can be caused by an error or an attacker
  - In the US, every county (many counties in each State) is responsible for its own voting technology
    - Thus, an attack against a particular machine will only affect votes cast on that kind of a machine.
- Electronic elections may lead to standardizing of election process

Opinions

1. The current Wintell PC environment is totally inadequate as a voting machine in public elections.
2. The current Internet is totally inadequate as a communications infrastructure in public elections.
3. The *level of threat* to *difficulty of attack* ratio for public elections in today's environment is too high.
4. Even if we could solve the technical issues, there are still social issues that are deal breakers for Internet voting in public elections.

Necessary precautions for computerized poll site voting

- care should be taken if voting machine are given network access
- Vote cartridges (for DRE systems)
  - Resistant to dropping, temperature change, magnetic forces
  - Should have physical world backup (paper)
  - Imagine a ruined/lost cartridge from a neighborhood with a particular, known demographic.
- Concentrate effort and funding on audit process, make sure neutral parties are involved, or balance with officials from opposing parties

Best advice might be to use optical scan with poll site tallying.