Integrity of Elections

Peter G. Neumann
Principal Scientist
SRI International ComputerSciLab
Menlo Park, CA 94025-3493
Neumann@CSL.sri.com
http://www.csl.sri.com/neumann
Tel 1-650-859-2375
Columbia University, 6 October 2008
The Importance of Elections

- In principle, fair elections are fundamental to democracy.
- In practice, elections have always been problematic, although moreso recently – with a rush to new systems that are poorly developed and inadequately vetted.
- The financial stakes are huge.
Prevalence of Weak Links

- Unfortunately, the entire process is vulnerable: voter registration, authentication, and authorization; voting, counting, certifying, recounting, resolving disputes; politics. People are very critical.
- Every step is a potential weak link: we actually have weakness in depth, not strength in depth.
A Paradigmatic Hard Problem

- Elections should have transparent integrity/reliability/accountability, oversight, untampered audit trails, definitive conflict resolution, uncompromised voter privacy, etc., throughout the entire process.

- Elections are inherently complex, even if conceptually simple. Many systems are seriously flawed.
All-Electronic Systems Are Risky

- Today’s all-electronic paperless voting systems lack integrity and auditability; they cannot resolve discrepancies due to fraud or undetected errors.
- Source code, data formats, data, evaluations, documentation are proprietary! “Trust us” is bad!!!
Simplistic Solutions Are Risky

- HAVA, EAC, voluntary standards (VVSG), evaluations (paid for by vendors) are all simplistic.
- Lever machines, punch cards, optical scan, touch-screens, people all have some problems.
- The rush to seemingly simplistic systems is fundamentally flawed.
Theory vs Practice

- Huge differences exist between research and practice/standards/evaluation/certification/use/...
- Many problems are nontechnical (absentee ballots, vote selling, voter coercion, politics, ...).
- System analyses are shocking!
- Crypto? Open systems? Low-tech (Rivest 3Ballot..., Chaum)?
California Secretary of State Debra Bowen commissioned review of 3 vendors: Hart Intercivic, Diebold (now Premier), Sequoia, with 3 reports each (red-team, source-code, documentation), plus 1 on accessibility. No ES&S.

http://www.sos.ca.gov/elections/elections_vsr.htm
NSF Center: ACCURATE

• A Center for Correct, Usable, Reliable, Auditable & Transparent Elections (ACCURATE): Johns Hopkins, Rice, U.C. Berkeley, Stanford, Iowa, SRI, with broad applicability to trustworthy systems overall.

• http://www.accurate-voting.org
Some ACCURATE Contributions

- UC Berkeley: Ka-Ping Yee thesis, starkly minimizes what must be trusted
- Rice: VoteBox, a tamper-evident, verifiable electronic voting system
- Participation in CA TTBR, Ohio, Sarasota, and more; VVSG review, EVT, new course materials, etc.
- http://www.accurate-voting.org
Some PGN Contributions

- Computer-related elections: http://www.csl.sri.com/neumann/#5
- 2006 Cal. State Senate testimony on needs for greater transparency: .../neumann/calsen06.pdf
- Risks in registration databases .../neumann/nrc-votpgn07.html
- Research on trustworthy systems .../neumann/chats4.html & .pdf
Past Election Problems

PGN, Illustrative Risks to the Public in the Use of Computer Systems and Related Technologies:
http://www.csl.sri.com/neumann/illustrative.html
Section on past election problems:
http://www.csl.sri.com/neumann/illustrative.html#25
Examples of Election Problems

- 1982: IN computer failed, patched
- 1984: Numerous suspect cases
- 1988: FL Senate race -14% dropoff
- 1992: OR, CA elections reversed
- 1996: MA chad reverses results
- 2000: FL bogus felons list; chad; Volusia Cty FL Gore -16,022 votes; 4-6M U.S. votes disenfranchised
- 2002: FL DREs switch votes
- 2003: 144K votes/19K voters: 5K;
- 2004: FL, OH, Swift-boating, ...
- 2006: Sarasota-13 18K undervotes
- 2008: Sarasota 10K votes e-vanesce, Palm Beach 2500 votes lost/found!
Contrasting Holistic Approaches

- Energy: future-oriented/short-sighted optimization
- Agriculture: natural/industrial
- Health care: prevention/“cure”
- Systems: principled/unprincipled

Energy

- Renewable resources (solar, wind, biomass, hybrids) can be viable if considered holistically.
- Fossil fuels are short-sighted, nonenvironmental, nonrenewable, contribute to global warming. Nuclear waste has long life.
Agriculture

- Sustainable agriculture uses natural fertilizers/pest-controls, crop rotations. It is healthful.
- Industrial agriculture causes soil depletion, toxic runoffs, worker and consumer health problems.
Health Care

- Alternative/preventive methods are holistic and environmental.
- “Modern” medicine seeks quick fixes that suppress symptoms rather than eliminating causes. It may be iatrogenic, trigger bacterial mutations, other effects ...
Holistic System Approaches

- We need principled trustworthy systems with sound requirements, structured architectures, and proactive design for usability, evolvability, pervasive assurance; selective use of formal methods.
- Elections desperately need this.
What Is Needed More Generally?

- Holistic analysis must address sustainable democracy, social equality, and environments; also proactive attention to aging infrastructures such as bridges, roads, levees, railroads, flood control, healthcare; perhaps most important: holistic education.
Some Computer-Related Conclusions

- We need proactive attention for computer-based infrastructures: trustworthy systems, transparency, oversight, and accountability.
- 20-20 foresight is much better than 20-20 hindsight. Priorities must be realistic and far-sighted.
- Elections are especially critical!
Lessons Still To Be Learned

- Reliance on misapplied technology usually increases risks.
- Privacy is often not appreciated until it is lost, and then may be impossible to recover.
- Privacy is difficult to ensure. Worse yet, it is often sacrificed in futile hopes for security.
- Eternal vigilance is required.
Technological Desires

- Better system architectures
- Better system engineering
- Better public-private cooperation
- Better technology in education
- Practical privacy-aware crypto
- Nonproprietary systems: open source/arch/doc/composability
- (Leads to permanent job security?)
Possible Forcing Functions?

- Market forces are inadequate.
- Incentives for open systems, open interfaces, open source?
- Stronger regulation & liability?
- Tax incentives?
- Better awareness of the risks of untrustworthiness; disasters?
- Maybe some or all of the above?
- But there are no easy answers.
Overarching Lessons

- Don’t overendow technology.
- Every would-be technological solution has some risks, and escalates the attacks.
- Attackers have many advantages over defenders. However, too often systems collapse on their own without provocation.