Previous Work on e-Voting

"The FEC Proposed Voting Systems Standard Update A Detailed Comment" by Dr. Rebecca Mercuri, submitted on 10 Sept. 2001.
http://mainline.brynmawr.edu/~rmercuri/notable/Papers/FECRM.html

This article is an analysis of the Federal Election Commission (FEC) proposed voting systems standards update. The article discusses much of the social and technical issues involved with e-voting systems. The author calls for a minimum set of performance benchmarks for electronic voting systems. This would only be possible through a Constitutional amendment creating minimal requirements for Federal elections. Such minimal requirements entail allowing straight-party ballots, the admission of blank ballots, the use of full-face ballots, and tabulation of proportional rather than highest vote results.
The article also focuses on the vendor aspect, revealing that the vendors are faced with conflicting requirements, and even more confusing is the aspect of each configuration for local and state elections need to be independently verified by testing authorities. Moreover, there exist no laws or requirements for checks and balances on vendor updates, equipment storage, equipment in transit, and equipment maintenance. Additional issues facing the vendor are design and code releasability questions verses the "trade secrets" argument.
Another unforeseen aspect of dealing with vendors is what happens when a vendor no longer is in business? Or when the vendor forces upgrading to the next product release?
The author is fiercely against the notion of Internet voting under any circumstances for numerous security failures on all systems: any hardware, software, and the leased network.
All software/firmware should be subject to examination. Also, there needs to exist an audit trail. Many consider the voting system similar to a banking system. However, the banking system has strong coloration between the user and the audits. A customer at an ATM uses a PIN, account card, has video cameras, and printed receipts to verify that that rightful customer accessed his/her account. Needless to say, that despite this requirements the banking system fails almost daily. Unlike the banks, the election system does not have an insurance program for the lost votes or malfunctioning machines. Furthermore, the voting systems must include a paper audit trail.
Another area where the FEC fails is the failure to use Trusted Computer System Evaluation Criteria (TCSEC). Nearly all systems with sensitive information are put through this rigorous Common Criteria process. There needs to exist both black box and white box testing of these systems. The area of Quality Assurance and Configuration Management has many failings. Who will store these machines? Who will properly verify they are working correctly? How will release updates work? Who has the final say of testing procedures? What about proper documentation for training, maintenance, or usability?
Finally, the issue of recounts is extremely important. There needs to exist a human readable output, to at least double check the machines results. "All voting systems carry with them some degree of error". When the result is within this degree, it is a TIE, a

revote is needed, not a recount.

"Voting-Machines Risks". Rebecca Mercuri. Inside Risks 29, CACM 35, 11 November 1992.

At the time of this article, NY was planning on purchasing 7000 Direct Recording Electronic (DRE) voting machines from Sequia Pacific. NY decided to go against the advice of the NY Bar Assoc., independent groups, and an independent consultant on voting systems and purchase the DRE system.
The risks from the DRE include the failure of 15 environmental/engineering requirements and 13 functional requirements including resistance to dropping, temperature, and vibration. The state of PA discovered that it "can be placed inadvertently in a mode in which the voter is unable to vote for certain candidates". At the time of this article, no laws existed to cover voting machines. Additionally, no laws in NY precluded convicted felons or foreign nationals from manufacturing, engineering, programming, or servicing voting machines.

"Opening a Can of Electronic Chad". Bill Sterner with Carol Schiffler.

In a recent review of three different electronic voting systems, not one produced a paper trail. There is no method to audit the validity of result. In comparison to a business, an accountant would need to see an audit trail for a persons income. No one would just take the computer's word for it. It is essential for voter confidence, contesting results, and democracy to have a readable, understandable audit trail.

"Florida Primary 2002: Back to the Future". Rebecca Mercuri. The Risks Digest, ACM Committee of Computers and Public Policy Forum on Risks to the Public in Computers and Related Systems. Volume 22: Issue, 24. 11 September 2002.

Dr. Rebecca Mercuri commented on how the FL 2002 Primary election went with all the money, new technologies, and promises issued. Many voters, including candidates, experienced delays from the new touch-screen machines not working. As a result, the elections were extended by 2 hrs, but some polling places did not receive the news, and closed early. In some counties, the machines just reset themselves, which caused all votes to be hand counted.
FL was warned about the machines, but decided to go ahead with the "trust us" leap of faith. The machines were not allowed to be tested during a trial run to verify that each candidate could successfully be selected, because of the vendor lawsuits. Moreover, the firmware was allowed to be updated just a week prior to the election, with no assurance of the process. Furthermore, the only form of a recount is the overall tally of the machines. There was no way of getting each vote, just a tally as a result.

"Press Releases: MIT vs Mercuri". Rebecca Mercuri. The Risks Digest, ACM Committee of Computers and Public Policy Forum on Risks to the Public in Computers and Related Systems. Volume 22: Issue, 26. 25 September 2002.

Dr. Rebecca Mercuri commented on the "flawed analysis" Caltech-MIT team results on the FL new voting technologies. She points out that they are comparing "apples to oranges" because it was comparing a General Election to a Primary Election. Not only do more people show up for the General, but also you have a greater chance that those people are not accustom to voting and produce the most errors. Moreover, she discusses how the average machine startup time is anywhere from 10 minutes to 23 minutes. So if each polling place had 10 machines, it could take more than an hour to get all machines operational. Some of the machines could not be turned up until 6:00 AM, as a "security" feature. The article also points out that since these communities are using the voting machines now, with no standards in place, how, will the current machines be upgraded whenever standards do occur? Dr. Mercuri requests that a moratorium on the purchase of any new voting system that do not provide voter-verification, hand recounts, physical paper ballots while appropriate laws, standards and technologies are developed to ensure secure, reliable, and auditable systems.

"E-Voting". Institute of Theoretical Computer Science, Cryptography and Information Security. www.crypto.ethz.ch/research/sdc/vote/index.html

According to this article, the three main requirements that should be met by an e-voting system are:

- Correctness – the computed tally must be correct as according to the cast legal votes
- Privacy – the cast vote of every voter must be kept private
- Availability – every entitled voter is able to participate in the election

This article also indicates that the e-voting system should be as efficient as possible for all participants. Specifically, the voter should only be required to interact once with the authorities, and the computation of the tally must be efficient even for a large number of voters. Another important requirement (proposed by Benaloh and Tuinstra) ofr an e-voting system is receipt freeness. This is defined as a scheme that prevents the voter from proving the vote he has cast, even when he wishes to reveal it. This can be seen as an extension to the privacy property, and it is especially important in settings where vote-buying and coercion may be issues.

"e-Voting Technical Security Requirements". CESG, Issue 1.0, X/10049/4600/6/21, 08 November 2002, http://www.localregions.odpm.gov.uk/elections/pdf/evoting.pdf

According to this paper, the following is a list of minimal security requirements that should be met by an e-voting system:

- Voter Authenticity – ensuring that the voter must identify themselves to be entitled to vote
- Voter Anonymity – ensuring that votes must not be associated with voter identity, unless warranted under law
- Data Confidentiality – ensuring the vote is secret
- Data Integrity – ensuring that each vote is recorded as intended
- System Accountability – ensuring that system operations are logged and audited
- System Integrity – ensuring that the system cannot be re-configured during operation
- System Disclosability – allowing the system to be open to external inspection and auditing
- System Availability – ensuring that the system is protected against accidental and malicious denial of service attacks
- System Reliability – developing the system in a manner that minimizes accidental bugs and ensures there is no malicious code
- Personnel Integrity – those developing and operating the voting system should have unquestionable records of behavior
- Operator Authentication and Control – ensuring that those operating and administering the system are authenticated and have functional access on the system strictly controlled

This paper also outlines several potential sources of attack against e-Voting systems including attacks coming from legitimate users, system operators, hostile individuals and organizations, and other individuals with "inside" access to the system. These attacks may come in the form of hacking, malicious software, Denial of Service (DOS) attacks, or Domain Name Service (DNS) attacks. Other threats to the overall security and reliability of an e-Voting system may be vote buying/selling, coercion, theft or forgery of election details, and deliberate repudiation of transaction. Some suggestions to counter these threats include the use of open auditing, and certain reporting procedures employed by the election officials.

"Revisiting legal and regulatory requirements for secure e-voting"
http://216.239.39.100/search?q=cache:MLO6l_0KIqwC:www.instore.gr/evote/evote_end/htm/3public/doc3/public/evote_paper_SEC_2002_2.doc+revisiting+legal+and+regulatory+requirements+for+secure+e-voting&hl=en&ie=UTF-8

This paper addressed various legal, constitutional, and security requirements that an e-voting system should satisfy. In order for an electronic voting system to be "fair" it must be as easy to access and use as the voting technologies that are already in place. For example, the ballots should be edited and displayed in a way that is similar to the layout of the paper ballots being used. Also, the structure and appearance of ballots shouldn't favor or discriminate against any of the participating parties. It is the opinion of the authors of this paper that the digital divide will not be overcome in the immediate future, and for this reason, e-voting should be a supplement to the current voting system, not a

replacement. Other issues that were mentioned include that of vote integrity and secrecy. In terms of vote integrity, a voter should only be able to vote once, and that vote must not be altered. Additionally, it should be infeasible to exclude a valid vote from the tabulation, and to validate a non-valid vote, and the outcome of the voting process must correspond to the votes cast. The secrecy of the vote must also be guaranteed during the casting, transfer, reception, collection, and tabulation of votes, and it should be impossible for anyone to link a voter to a particular vote. Similarly, a voter should not be able to prove that they voted a certain way. The system itself must also be reliable in the sense that voters, parties, and candidates must be ensured that there has been no malpractice. This requires that all operations must be monitored, while secrecy is preserved, and the entire infrastructure (including source code) as well as every system's functionality must be logged. All parties should have the opportunity for equal access to the elements of the voting procedure, in order to be able to establish its proper functioning.

Mohen, J. Glidden, J. The case for Internet voting. In *Communications of the ACM*, January 2001.

The Case for Internet Voting

Uses the Arizona Democratic Party presidential preference election held in March 2000 as a case study. It was held between March 7-11 and was the first time voters from anywhere in the world were able to cast their ballots from the location of their choice. *Election.com* was the company selected to conduct the primary and they also wrote this article (the authors are the CEO and VP for public affairs for the company respectively), so they are in a unique position to comment on the pros and cons of Internet voting.

Because there were no clear guidelines for the election process at the time of this election, it was up to the implementers to come up with procedures and protocols.

One goal was to increase access and voter participation. They implemented an outreach program to inform voters of the technology, and ensure equal access to the ballot. They sent out 849,000 sealed first-class mail notices to registered Democrats. The mail was printed in both English and Spanish and included a unique voter identification number, a tear-off ballot to enable vote-by-mail from March 7-10. Unregistered voters were also allowed to register at the poll sites.

To increase awareness and accessibility, they increased the number of physical polling places from 92 to 124, and advertised extensively in print, broadcast and radio outlets. *Election.com* invited several third party groups to attend the election.

Security mechanisms:

Voter Authentication

- Issued seven-digit alphanumeric PINS.
- Voters were given two questions out of five possible confidential choices, such as: the last four digits of a SSN, or a Date of Birth.

- The system voided ballots from reuse once they were cast (or if the name or address was incorrect, or if they requested a mail-in ballot).
- The voter had to confirm reading a statement relaying the penalty for misuse or falsifying information.
- Digital signatures were used to authenticate the servers to one another.

Ballot Protection and Privacy

- KPMG generated a public/private key pair of which the public key was used to encrypt the ballots. *Election.com* never had access to the clear text ballots.
- The voter's ID and ballot were separated and stored in two different relational databases, so that voter identities would remain anonymous.
- The two tables were encrypted, and the one with the ballots was sneaker-netted to the KPMG server for decryption and counting.

Preventing wholesale insider fraud

- Their engineers and technicians worked on the stored procedures separately…yada yada yada…ensured ballots were compartmented…
- Audited data – who voted, not who they voted for
- Audited hardware – database server audit logs
- Audited source-code – using commercial source-code management software.

Preventing DOS attacks

- DDOS attacks were attempted, but system was designed to deflect these attacks
- Used Intrusion Detection Software to filter out such attacks….
- Also allowed Internet voting only on the four days preceding the actual election day (March 7-10).

Virus/Trojan Horse attacks

- The authors recognize these types of attacks, but they equate the possibility of such an attack with one against an e-commerce system.
- They also suggest that the risk is acceptable if the elections are small enough.

Application Security

- The voting software was designed with layers, so there would be more layers of protection for the data (votes).
- The Server's OS and applications (web-servers) were patched.
- Data was replicated to a standby server.
- A card key and thumbprint were required to gain access to the site.
- Each component was designed to have at least one failover companion.
- Failover didn't go smoothly for one of the routers, which didn't allow voting for one-hour on March 7th.

<u>Lessons Learned:</u>

- Help desk lines were flooded around the clock
- Older browsers could not handle the encryption requirements.

- Several Macintosh users were not able to cast their votes online.
- Ensuring right to vote for people with disabilities is tough.
- Internet voting at the polling place adds little value to the voting process, while adding substantial cost to the election.
- Voters prefer multiple voting options.

Policymakers must make decisions to enable Internet voting in a way that retains the public trust. It should reflect equal or improved levels of security, integrity, and transparency when compared to today's system.

"A Better Ballot Box". Rebecca Mercuri. IEEE Spectrum. October 2002. pp. 46–50.

This article gives great detail on the current reality of electronic voting systems. Many voters think that technology will save the day, but in reality the current voting systems can cause less accountability, poorer reliability and greater opportunity for widespread fraud. The Mercuri method of voting incorporates a kiosk machine that prints out a human and machine-readable ballot for voting verification. The voter has the chance to inspect the choices and choose to modify, accept or delete ballot. This step in the voting system is crucial to instill voter confidence and system accuracy. Also, the article goes into great detail describing the need to verify the systems in place. We can't have this "trust us" way of thinking. There needs to exist a very real paper trail to ensure that technology has not compromised voter intent. Many minimum requirements do not exist, leaving the vendor to create them as the go. This causes many security, practical and unforeseen consequences that are costing states millions of dollars.

Neumann, Peter G., *Security Criteria for Electronic Voting*, 16th National Computer Security Conference Baltimore, Maryland, September 20-23, 1993,
http://www.csl.sri.com/users/neumann/ncs93.html

According to Mr. Neumann, the following is a list of generic voting criteria that voting systems should satisfy:

- System integrity
  - The computer systems must be tamperproof
  - System changes must be prohibited throughout the active stages of the election process
  - System bootload must be protected from subversion that could otherwise be used to implant Trojan horses
  - Above all, vote counting must produce reproducibly correct results
- Data integrity and reliability
  - All data involved in entering and tabulating votes must be tamperproof
  - Votes must be recorded correctly
- Voter anonymity and data confidentiality

        - The voting counts must be protected from external reading during the voting process
        - The association between recorded votes and the identity of the voter must be completely unknown within the voting systems
    - Operator authentication
        - All people authorized to administer an election must gain access with nontrivial authentication mechanisms
        - There must be no trapdoors that could be used for operational subversions
    - System accountability
        - All internal operations must be monitored, without violating voter confidentiality (monitoring includes votes recorded and votes tabulated, and all system programming and administrative operations such as pre- and post-election testing)
        - All attempted and successful changes to configuration status (especially those in violation of the static system integrity requirement) must be noted
    - System disclosability
        - The system software, hardware, microcode, and any custom circuitry must be open for random inspection at any time (including documentation)
    - System availability
        - The system must be protected against both accidental and malicious denials of service, and must be available for use whenever it is expected to be operational
    - System reliability
        - System development (design, implementation, maintenance, etc.) should attempt to minimize the likelihood of accidental system bugs and malicious code
    - Interface usability
        - Systems must be amenable to easy use by local election officials, and must not necessitate the on-line control of external personnel (such as vendor-supplied operators)
        - The interface to the system should be inherently fail-safe, fool-proof, and overly cautious in defending against accidental and intentional misuse
    - Documentation and assurance
        - The design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and consistently documented
        - Documentation must also describe what assurance measures have been applied to each of those system aspects

A suggestion as to how to improve the system's integrity was to use "locally non-modifiable read-only and once-writable memories, particularly for system programs and preset configuration data, respectively". Another suggestion was to include the use of redundancy to improve security and reliability, as long as it doesn't introduce

further complexity and potential vulnerabilities. This article also mentioned that in addition to meeting this list of security requirements, the system must also conform to applicable election laws.

Conclusion: there will always be a tradeoff between certain functional and security requirements

- "The requirement for voter confidentiality and the requirement for nonsubvertible and sufficiently complete end-to-end monitoring are conceptually contradictory. It is essentially impossible to achieve both at the same time without resorting to complicated mechanisms, which themselves may introduce new potential vulnerabilities and opportunities for more sophisticated subversions"

Report of the National Workshop on Internet Voting (NSF)

This paper addressed several of the system vulnerabilities that are present in an e-voting system that uses the Internet. Such vulnerabilities include: defense/verification against insider fraud for poll site voting, general defenses against Trojan horse attacks and malicious use of remote control software, specific design of secure voting platforms and networks, defenses against denial of service attacks, and defenses against the use of fake voting sites. For poll site voting it is suggested that the system be designed so that it can function properly in the event that the connection is interrupted between the poll site and the server. This might be accomplished by incorporating the functionality of a DRE machine, such that the voting client uses the Internet to transmit the votes when it is available. Some important legislature mentioned in this paper includes the set of voluntary standards for voting systems proposed in 1990 by the National Association of State Elections Directors (NASED), and the 1993 National Voter Registration Act, that limited the amount of information states could require in the registration process and made it more difficult for election officials to purge registration lists.

Rubin, A. *Security Considerations for Electronic Voting over the Internet*

In the wake of the closely contested elections of 2000, there is an increased demand for better election practices. As a result, there is also a loss in the public's confidence of the election process. Many people see a solution to these problems in technology. Unfortunately, if the technology used isn't implemented very carefully, we run the risk of losing the ability to participate in the election process.

This paper focuses on the security issues related to using the Internet and currently prevalent technology to perform Electronic Voting.

<u>Voting Platform</u>

The first part of an Internet voting system lies on the machines with which the voters directly interact. For the article, the author focused on the most common platform, Intel machines running the Windows operating system and participating from home

These platforms are very susceptible to attacks from malicious users who are not necessarily very technically skilled.

Malicious Payload

The author mentions the variety of possible attacks against Wintel voting platforms, and goes into detail about BackOrifice and the Chernobyl virus. BackOrifice (BO2k) is a remote control program that is very difficult to detect, and would enable a malicious user to view the voting process as well as change the voters intention. The virus is mention because it was programmed to go off on a certain date, and on that date, it damaged computers all around the world pretty severely.

Delivery Mechanism

In this section, the author outlines how easily the malicious payload can be installed on a potential voter's computer. People's computers are not typically physically secured, so anyone who has access to the machine can install software onto it. But, this avenue of attack pales in comparison to remote automated delivery used by email viruses and worms. In fact any software, including the operating system, can have exploitable bugs or hidden Trojan horses just waiting to be activated and disrupt the election process.

The Communications Infrastructure

Denial of Service Attacks can disrupt the communications infrastructure. They make computer systems completely unusable, so even if oth end of the network are working, there may be no path between them. These attacks can be found on the Internet is ready-to-use form and activated easily by script-kiddies.

Social Engineering

Social engineering attacks involve conning people into compromising their security. There are a number of ways an adversary could fool people into thinking that they were communicating with the real election server. One way is to set up a fake voting site and direct users to it. The Domain Name System could be fooled into directing users to a malicious site.

Specialized Devices

There exist specialized devices, such as cryptographic smart cards that could make the voting procedures more secure. However, they can be a significant cost to the end users, and can become the equivalent of a poll tax, which cannot by law be required in order to vote. Even with this technology, the underlying computer still must be trusted to behave as expected.

According to the author, there is no way to carry out Internet voting securely, given the insecurities of the host platforms and the vulnerability of the Internet to manipulation and denial of service attacks. To solve the problem of host insecurity, some hardware support as defined by the Trusted Computing Platform Alliance must be implemented to enable a trusted path between the voter and the election server. He doesn't mention a possible solution to the problems of the Internet.

CalTech/MIT Voting Technology Project, July 2001

This report summarized the basic steps in the voting process as: registering to vote, getting to the polls, casting a ballot, counting ballots, and certifying the vote. More specifically, the four components of the US voting system are: voter authentication (voter registration), communication of voter preferences (balloting), the counting of these preferences (ballot counting techniques), and the security of the voting system (secret ballots). Several issues with the current voting scheme, covering varying steps of the voting process, were raised in this paper. For example, for the most part, local governments have been given the authority for administering elections – should this be changed? Also, every county and state has its own voter registration system , but should they be centralized? Should congress impose uniform technologies for casting and counting votes in national elections? Should the time period allotted for voting be extended? Should there be various languages on ballots? All of these questions are important to consider when designing an e-voting system, and each should be researched to determine if they would lead to an improvement in the overall voting process. Some additional issues that were discussed include:

- Preventing voters from over-voting
- Should provisional ballots be required/allowed?
- Should poll workers have to be registered in the precinct where they work?

This paper also provided a lot of insight into previous/current work in the area of electronic voting. For example, information was provided that indicated optical scanners perform relatively well (compared to other voting techniques), and that while Riverside, Ca had good experiences with touch screens, Beaver County, PA and several counties in New Mexico did not.

This paper also dealt with the problems with registration process and possible improvements. According to this paper, the 5 standards that need to be met by voter registration system are:

- all info must be accurate and complete
- info must be immune from fraud
- info must be dynamic and up to date
- info must be usable by the election officials at the polling site
- must be easy for voters to register

It is also suggested that a system be developed to allow voters to check their registrations (done in North Carolina), and to have some sort of computerized voter registration (done in Michigan and Oklahoma). In Orange County, Fla the county/state's registration DB is accessible at each polling site (registration info is on a CD, and a laptop is leased to each polling site). Another suggestion is to have some sort of numerical id on voter's registration.

California Internet Voting Task Force

- Ballot integrity and secrecy can be protected while ballots are transmitted over the Internet through the use of digital signature and encryption technology. All identifying information used to electronically verify the identity of a voter shall be stripped from the ballot prior to the tabulation of the votes to ensure the secrecy of all Internet ballots.
- Federal Voting Rights Act (1965) - enacted for the purpose of ensuring that no voting qualifications or procedures are imposed that would have the effect of abridging or denying voting rights to citizens based on account of race or color.
- This task force recommends that the adoption of Remote Internet Voting technology in the near term ought to be modeled on the California absentee ballot process. By requiring a voter to request an electronic ballot on paper, election officials will be able to compare the voter's signature on the electronic ballot application with the voter's signature on the voter registration card.
- Internet Voting Machines must be secured from attacks on the operating system. Potential computer attacks include malicious "Virus" or "Trojan Horse" computer code which could affect access to or the integrity of a voter's ballot. In this first stage of Internet Voting, the securing of the machines would be completed by election officials.
- The recent ABC news nationwide poll indicates that currently only 19% of the population of Americans who are over 65 would support Internet voting even if it could be made secure from fraud. These numbers indicate that any Internet voting system would have to make an effort to increase the comfort level of the elderly population
- An Internet voting system must include a process by which the Internet voter may write-in the name of a candidate for an office and vote for that candidate if he or she chooses to do so