The Risk of e-Voting

Thomas W. Lauer
School of Business Administration, Oakland University, Rochester, USA
lauer@oakland.edu

Abstract: World wide, there are various proposals for automating manual voting processes. This paper considers two different e-voting schemes, Internet voting and direct recording electronic (DRE) voting systems, explicitly focusing on risk to the integrity of the voting process. Fair elections must assure voter authentication, vote confidentiality and integrity, and the ability to audit the election. E-voting poses special challenges. The paper analyzes security risks that may threaten e-voting schemes and makes recommendations.

Keywords: Internet voting, e-voting, direct recording electronic voting, IS security, risk analysis, voter fraud

1. Introduction

On the surface, it may seem that automating manual voting processes through the use of information technology would be a straightforward application that would improve efficiency and would avoid problems that plagued the 2000 US presidential election. This paper considers two different e-voting schemes, Internet voting and direct recording electronic (DRE) voting systems. At present, there are a number of trials of these systems being carried out worldwide. Proponents of e-voting have argued that it will have the following salutary effects: increased participation for disadvantaged communities, an antidote to voter apathy, greater voter convenience in terms of voting time and location, access for people with disabilities, money saving, and greater accuracy (Mohen and Glidden 2001). However, a number of authors have raised cautions that e-voting poses a number of security issues (Mercouri 2002; Neumann 2001).

Systematic approaches to assessing and managing security risks in organizational contexts such as the OCTAVE℠ approach (Alberts & Dorofee 2003) identify the assets to be protected, the risk to those assets, and the cost and effectiveness of protective measures. The participation of organizational stakeholders is essential since they have explicit knowledge of the relative importance of specific assets within the organization. An analogous approach can be taken for the analysis of society wide systems such as a voting system. However, a much broader view of stakeholder interest and potential risk must be incorporated into such an analysis. Among the assets that must be included are those associated with determining the winner of a specific election as well as the public confidence in the overall fairness of the election process. Some requirements for a fair voting system include assurances with respect to: the voter (authenticity and anonymity), the data (confidentiality and integrity), the system (that it can be audited, inspected, is available, is reliable) and personnel operating the system.

As with other security decisions, those for e-voting systems involve trade-offs. What assets are protected at what cost? Although social costs are important for any security decision, they are of prime importance for e-voting systems. Certain benefits are claimed for e-voting by proponents while opponents argue that threats to the fairness of the election process make the risk of these systems too great. This paper will show where the trade-offs lie. The remainder of the paper proceeds as follows. The next section gives a brief summary of the OCTAVE℠ method. Next is a discussion of what assets are at risk in a democratic election and what security measures are required. Following this, a risk assessment examines risk components (magnitude of loss, likelihood of loss, and exposure to loss) in DRE and Internet voting regimes. The final section offers a commentary on the prior analysis.

2. Security risk analysis

OCTAVE℠ stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation and is a process for assessing information security risk described as being comprehensive, systematic, and

ISSN: 1479-439X

context driven. It includes three phases: 1) building asset based threat profiles, 2) identifying infrastructure vulnerabilities, and 3) developing security strategy and plans. Threat profiles include a description of the asset, identification of the actor and the actor's motive, explanation of the means by which the asset is accessed, and a description of the outcome. See figure 1 for a depiction of generic threats. Infrastructure vulnerabilities should take into consideration known vulnerabilities such as susceptibility to denial of service attacks. Risks are evaluated by analyzing interrelationships among assets, specific threats, and vulnerabilities.

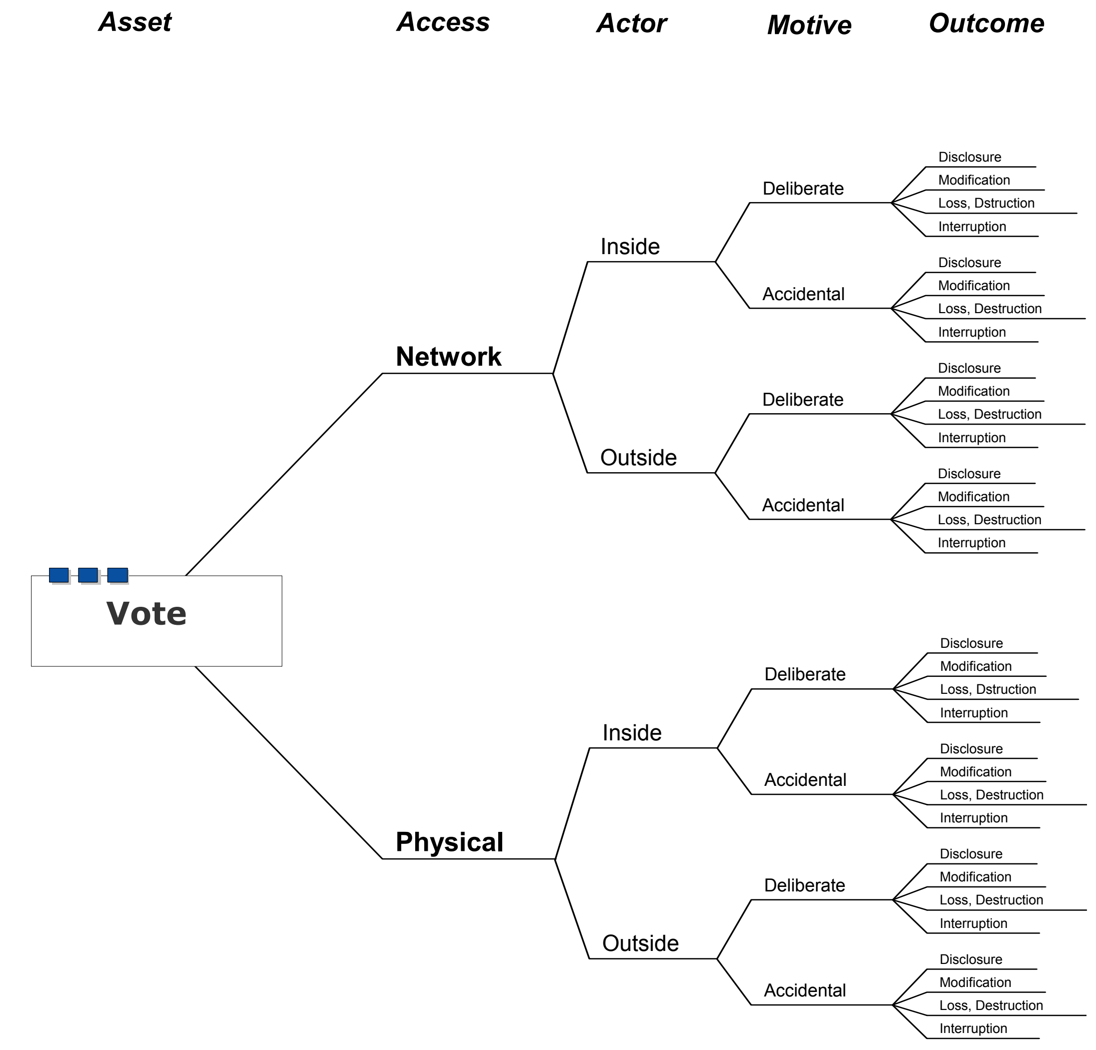


Figure 1: Generic Threat Model

Each of the three phases has outputs resulting from implementing the OCTAVE℠ method. Phase #1 produces an identification of critical assets, a specification of security requirements, a description of threats, a description of current security practices, and an identification of missing or inadequate practices. Phase #2 results in a depiction of the key technological components and the identification of technological vulnerabilities. Phase #3 yields a risk assessment for each threat, the development of a protection strategy, and a plan for risk mitigation.

Among the defining characteristics of a democracy are universal suffrage among adult citizens and fair and regular elections. In order for elections to be fair, the voting process must provide certain guarantees. To assure fair elections, security provisions must account for individual voters, the vote itself, the voting system (voting technology and voting processes), and personnel responsible for carrying out elections. Thus in a democracy, elections, their processes, and the individual vote are all assets to be protected.

The voter must be authorized and authenticated. National elections require that eligible voters be citizens of a certain age. In the US, most states bar convicted felons from participation in public elections. In addition, in order to prevent coercion and vote selling, the voter must be able to vote anonymously, i.e. votes must not be associated with voter identity. Votes must be assured of confidentiality (being secret) and integrity (the vote is recorded as intended). Voting technology must support logging so that its operations can be audited. Its configuration must be open and controlled so that it can be inspected and can't be modified while operating. In addition, it must be reliable and available so that it operates without error while an election is taking place. Personnel responsible for developing, operating, and maintaining voting technology should have records of impeccable behavior as should those charged with running the election.

Democracy depends in part on the trust of the citizenry, trust in public institutions such as elections. Thus, the institution of elections is an asset in a democratic society. Threats to the perception of fairness, for example through disenfranchisement, are also pertinent to election security.

3. Comparing DRE voting and Internet voting to the status quo

3.1 US election and voting machine history

The first elections conducted in the United States established eligibility based on land ownership. Between 4 – 6% of eligible voters participated in the first few presidential elections. In the 1830s, land ownership requirements were relaxed and a high point with respect to participation of eligible voters was reached in the 1840 presidential election with 80% of white males participating. The 15th Amendment to the Constitution gave blacks the right to vote, and the 19th Amendment, granting voting rights to women, was ratified in 1920. Since then, there have been a number of voting rights laws passed. The Civil Rights Act of 1957 and the Voting Rights Act of 1965 abolished discriminatory literacy tests and other procedures that effectively barred a prospective voter based on race. Most recently, the National Voter Registration Act of 1993 is aimed at increasing voter participation in elections (Delk 2001).

The word ballot comes from the Italian for ball, *ballota* and refers to an ancient election technique where balls were placed in a container to signify votes. Early paper ballots could have been mere slips of paper, newspaper advertisements, or a printed party ticket listing a party's endorsed set of candidates. These ballots and accepted voting procedures did nothing to guarantee voter privacy or voting more than once. In 1888, the Australian Paper Ballot was used for statewide elections in New York and Massachusetts. The Australian Ballot has three characteristics, officiality, consolidation, and secrecy; officiality because the ballot was designed and printed by the state, consolidation because it listed all candidates from each party, and secrecy because voting took place in a voting booth. As Jones (2004) observes, "A properly administered Australian paper ballot sets an extremely high standard that any competing election technology must match." He goes on to note the high cost of paper ballots and hand counting in elections where there are large numbers of candidates.

Around 1890, two voting technologies were introduced, the lever voting machine and the punched card. Lever voting machines keep a running total of votes cast by means of a mechanical wheel. Thus they are not amenable to recount. Punched cards can be used with voting booklet that lists the candidates and a stylus for punching holes for the vote. Vote counting is automated through the use of a punched card reader or a tabulating machine. The problem with recounts is they must account for partially punched holes so the intention of the voter is ambiguous. Although the 2000 US presidential election introduced most of us to "chadology", there had been warnings regarding this technology dating from the 1960s. Optical mark-sense scanners were first used for elections in the 1960s. These devices enable automated counting, manual recounting, and recounts.

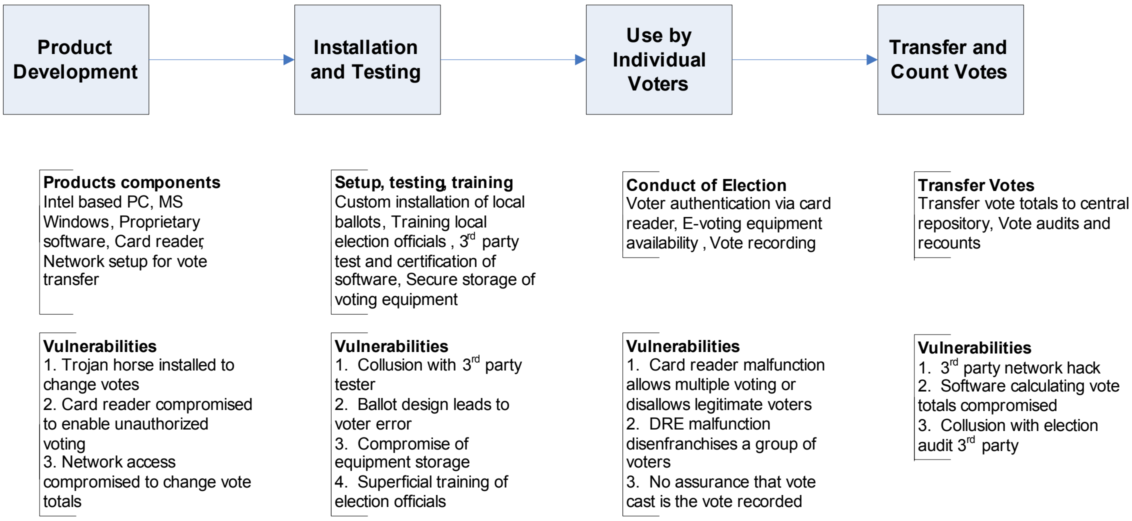
A typical DRE voting system consists of a Wintel PC equipped with a touch screen packaged in a secure case to prevent plugging in a mouse or keyboard. It plugs into a network hub with an uninterruptible power supply and sits in a voting booth with a privacy screen. In effect, it is a computerized lever voting machine. Voters go to their precinct where they are authenticated and are typically given a smart card or PIN that enables them to access the machine. Votes are recorded and kept within the voting system and subsequently loaded into an election management system. Thus it does not permit recounts.

3.2 Internet voting

The first Internet vote was cast by US astronaut David Wolf who was allowed to vote by e-mail from the space station Mir in the 1997 Texas election. The ballot was e-mailed from his local election office to Johnson Space center, then to Russia's space agency before being uplinked to the space station. Since then, Internet elections have been conducted in Alaska, the Arizona primary, and most recently in the Michigan primary. The Internet voting system used in Arizona included the following features: (1) a provision for authentication (a PIN mailed to an eligible voter), (2) encryption of the vote with a public key on the client machine with the private key held by a trusted 3rd party, (3) transmission of the vote to an election.com server using a SSL encrypted pipe, (4) separation of the voter identity from the vote into two tables. Audit logs tracked who voted and another audit logged monitored access to the database server. Only the trusted 3rd party (in this case KPMG) was authorized to decrypt the votes (Mohen and Glidden 2001).

3.3 Voting system life cycle

Many discussions of voting system security vulnerability fail to consider the entire voting system. In addition to the hardware and software that make up the voting equipment, the system includes election workers, voters, and is deployed in a variety of physical environments. Election workers are often volunteers whose skill with technology can vary widely. Similarly, voting technology that assumes a level of technological literacy on the part of the individual voter will potentially be susceptible to error. A security assessment of election equipment that only considers hardware and software without examining its use in real contexts may conclude that the equipment is satisfactory. Considering the larger system including election workers and voters will require analysis of procedures with a focus on fair voting criteria – anonymity, confidentiality, integrity, and auditability.



Products components
Intel based PC, MS Windows, Proprietary software, Card reader, Network setup for vote transfer

Vulnerabilities
1. Trojan horse installed to change votes
2. Card reader compromised to enable unauthorized voting
3. Network access compromised to change vote totals

Setup, testing, training
Custom installation of local ballots, Training local election officials , 3rd party test and certification of software, Secure storage of voting equipment

Vulnerabilities
1. Collusion with 3rd party tester
2. Ballot design leads to voter error
3. Compromise of equipment storage
4. Superficial training of election officials

Conduct of Election
Voter authentication via card reader, E-voting equipment availability , Vote recording

Vulnerabilities
1. Card reader malfunction allows multiple voting or disallows legitimate voters
2. DRE malfunction disenfranchises a group of voters
3. No assurance that vote cast is the vote recorded

Transfer Votes
Transfer vote totals to central repository, Vote audits and recounts

Vulnerabilities
1. 3rd party network hack
2. Software calculating vote totals compromised
3. Collusion with election audit 3rd party

Figure 2: DRE life cycle showing security vulnerabilities by stage

Figure 2 shows a voting system life cycle. At each stage, there are products and procedures that may be vulnerable to error or compromise. The figure also shows specific vulnerabilities relevant to each stage of the life cycle. The effectiveness of the security protecting the voting system can be measured against the extent to which it ensures the criteria for fair voting are met. From this standpoint, it doesn't matter whether failures to satisfy a criterion result from fraud or error. For example, malware that changes votes and interfaces that are incomprehensible both fail to count the vote as intended.

3.4 Security threats to DRE voting systems

As noted above, the integrity of the results generated by the DRE voting system is dependent on the correctness, robustness, and security of the software in the voting terminal and the procedures for tabulating the results. If the voting system software is flawed, an election can be compromised by voters or malicious insiders. Malicious insiders could include election officials, software developers, those responsible for DRE system maintenance, or even developers of the operating system underlying the DRE system (Kohno et al. 2003). A malicious insider working for Microsoft could install software that was activated by the election date and changed 10% of the straight ticket votes for one party. By using code obfuscation techniques, this would be very difficult to discover (Jones 2001). Election procedures are also important. Tampering with election equipment can occur if the physical security of DRE equipment is inadequate. Once a DRE unit has been certified for use, procedure should be in place to ensure that new software is not loaded onto the machine. Examples of security threats to DRE voting systems and their potential consequences can be found in Table 1.

Table 1: Threats to Direct Recording Electronic Voting Systems

Threat	Consequence	Likelihood	Countermeasures
Trojan horse installed by DRE vendor	Wholesale election compromise	Unknown – consider gaming industry as reference	Detection very difficult especially when code obfuscation techniques used
Trojan horse installed by Operating System vendor	Wholesale	No known example, but theoretically possible	See above
Trade secrecy	Prevents examination and adequate testing of software	Certain	Require Open Source system components and vendor source code inspection and testing
Lack of standards	Prevents adequate testing of DRE Voting system	Certain	Develop standards (a slow process)
Lack of configuration oversight	Configuration change could introduce new voting compromises	Known problems with configuration oversight	Stronger legal sanctions – but oversight is expensive
Buggy software	Potential for multiple voting, loss of voter privacy	Unknown	Better testing and certification of DRE voting systems
			The most effective countermeasure for many of the above problems is to use a voter verified audit trail

3.5 Security threats to Internet voting

Internet voting systems pose numerous security threats the most significant of which have to do with vulnerabilities of the PC platform and vulnerabilities associated with the Internet itself. Client PCs could be located in voters' homes or in public or commercial establishments such as libraries or cyber cafés. Assuring that all possible PCs are free of malware is not practically possible. In addition, there can be no assurance of voter privacy as there is with Australian Ballots. Individuals in abusive relationships could be coerced to vote a particular way. If a person's PC is used to cast a ballot, does it then become a polling place subject to election law? In addition, it may not be possible to prevent widespread vote selling. Since this could be done from an offshore location, jurisdictional sanctions may not exist. There are also Internet infrastructure problems that make voting susceptible to denial of service attacks. These could be carried out selectively to disenfranchise voters in particular neighborhoods. Once an election is over, it is not possible to run it again under current laws governing elections.

In addition to problems with client PCs and the Internet, there are problems having to do with vendors of I-voting systems many of which are the same as those that pertain to DRE systems. The same potential for insider attacks exists and the same problems having to do with closed source systems makes it difficult to develop appropriate standards, testing, and certification for these systems. Finally, there is a problem with using a trusted 3rd party. One needs only to recall the role played by Arthur Andersen in the Enron scandal. See Table 2 for some example security threats to I-voting systems.

Table 2: Example Threats to Internet Voting

Threat	Consequence	Likelihood	Countermeasures
Denial of Service	Disenfranchisement	Common, occurred during Canadian Internet election	No simple countermeasures
Trojan horse spyware to change or monitor votes	Vote theft, loss of privacy	Widely available tools for this	Detection difficult. Individual PCs can be protected, but assuring compliance difficult, especially for public PCs.
Automated vote buying	Compromise of election	Likely since there exist organizations set up to do this.	None. Organizations may exist outside country's jurisdiction
Insider attack on voting system	Compromise of election	Insider attacks are common in commercial settings.	Separation of duties, adequate documentation, control over physical assets, independent audits,
Virus specific to Internet voting system	Vote theft, privacy loss, disenfranchisement, compromise of election	Unknown	Very difficult since such a virus would have no prior history
Spoofing	Vote theft,	Common and easy	Can be launched from anywhere. Made difficult by use of encrypted PIN

4. Risk analysis

The OCTAVE℠ method provides a practical means of identifying assets and threats to the assets. A practical means of supplementing our understanding these security threats risk considers magnitude of loss, likelihood of loss, and exposure to loss (MacCrimmon and Wehrung 1986). For elections, the magnitude of loss is partially determined by the type of election; local elections concerning bond issues have a much lower potential magnitude of loss than do national presidential elections. In this section, we will focus on national elections.

A recent analysis, Kocher and Schneier (2004) is useful for estimating the magnitude of loss. They argued that stealing control of the U.S. House of Representatives is conservatively worth $100 million and that changing a single race is worth $3 million. They consider two scenarios, one in which physical security for individual voting machines is wanting, and another where voting machines are used in 25% of polling locations and there is widespread corruption of the machines through insider fraud. In the first case, they estimate the value of swinging the votes on an individual machine (in a close race) at $5,000. In the second case, they estimate the overall value to be at least $100 million. Presumably fraud that changes the balance in the Senate or the Presidential election would be worth even more. While these numbers seem large, a monetary estimate of loss from election fraud fails to include potential damage to social institutions and public trust and therefore is a serious underestimate of the magnitude of loss.

Estimating the likelihood of loss is really an estimation of the likelihood that someone will try to swing an election by attacking the DRE or Internet voting system. There is a variety of relevant evidence including direct evidence with DRE voting, historical evidence pertaining to election fraud, and evidence of attacks on essentially similar systems in other contexts. Likelihood depends on both the motivation of the attacker and the vulnerability of the technological system.

There has been considerable documentation of e-voting errors in the U.S. press during the past year, especially as the Presidential election looms near. In a reaction to the 2000 election fiasco with recounts depending on the interpretation of hanging chads, many state election commissions opted to replace punch card systems with DRE e-voting systems. DRE systems have been used in state primary elections and special elections. One special election in Florida to elect a Congress person was decided by 12 votes. The DRE systems used recorded 134 undervotes, a highly unlikely event since that was the only contest on the ballot. Nonetheless, the secretary of state, Glenda Hood certified the election claiming the voting equipment functioned properly. Considerable controversy has surrounded Diebold Corporation, makers of the AccuVote machine. Diebold's machines have been decertified in California and they may face criminal charges. These charges stem from using equipment that had not been certified (Zetter 2004). In the 2004 Maryland primary, machines in three counties wouldn't let voters vote for senator (Kantor 2004). Subsequently, Diebold officials admitted that the software used for the March, 2004 Maryland primary elections was not certified as required by law (Schade 2004). Internationally, there have been similar controversies. In Venezuela, the government had purchased a 28% share in Bizta Corporation, a firm that produces the software for the DRE voting systems that were to be used in the recall election of Venezuelan President Hugo Chavez. Omar Montilla, a senior government official representing the government's 3,000,000 shares on the Bizta board resigned after being exposed by the Miami Herald article. E-voting machines were used in India's recent national elections. A New York Times article describes how political hooligans took over voting booths in small villages and stuffed the electronic ballot boxes. This technique, described as "…a new version of a storied Indian electoral trick…" is known as 'booth capturing' (Rohde 2004). For other examples of e-voting security failures see Neumann (2001).

Tables 1 and 2 show some examples of techniques for compromising DRE voting and Internet voting. One thing to note about these examples is that most are carried out by insiders. One industry that has developed security methods for similar insider attacks is the gambling industry. Gambling industry motivation for strong security stems from their perception of the risk of fraud. The Nevada Gaming Control Commission has the following procedures in place for regulating gaming equipment:

1. Government access to all gaming software,
2. Random spot checks of gaming equipment,
3. Rigorous testing and updating of standards for equipment,
4. Background checks for companies selling gaming machines and for their employees,
5. Arms length relationship between manufacturers and testers of equipment, and
6. Procedures for citizen complaints and recourse.

The absence of similar protections in the e-voting industry can only serve to increase the likelihood of errors and/or fraud that would compromise an election.

Finally, risk analysis considers exposure to loss. As with other industries that have replaced manual systems with computerized systems, the introduction of e-voting systems raises the potential of moving from localized fraud and voting error to widespread fraud and voting error. For national elections or even state elections where there are many polling places, adherence to Australian Ballot principles makes widespread fraud difficult. In contrast, by introducing software that biases voting systematically in DRE systems or Internet voting systems widespread exposure markedly increases risk. The difference is between local fraud and wholesale fraud. In a democratic society, this specter of election corruption is a threat to all. Exposure can also be understood through those who would threaten an election. Kocher and Schneier (2004) identify adversaries as system developers, election insiders, foreign governments, radical extremists, and partisan operatives. Those exposed include any who might suffer at the hands of members of that list of adversaries.

5. Commentary

Proposed introduction of DRE systems has provoked heated disputes both in the US and elsewhere. Some DRE system vendors have insisted that their software not be scrutinized by inspectors maintaining that closed source or "security by obscurity" is the best form of protection against maliciousness. Recently, using publicly available source code from a firm that sells DRE voting equipment to states, Kohno et al. (2003) identified a number of flaws in the software that could enable voters to cast multiple votes without traceability or access system administrative functions. Weakness of these systems is further borne out by the fact that DRE systems have on occasion produced erroneous results (Cranor 2002) proving that the software is flawed. The issue of open source for e-voting software is currently an issue in Holland and Ireland as well (Libbenga 2004).

The most practical immediate solution (one that would temporarily forestall the open/closed source issue) is to use a "voter verified audit trail" (Dill et al 2003). One example is the Mercuri method (Mercuri 2002) in which the DRE system prints the voter's ballot behind a transparent pane. If it's correct, the voter deposits it mechanically in a ballot box. If not, a poll worker is called, the ballot is voided, and the voter is given another chance to vote. In cases of discrepancies, the paper ballots take precedence over the electronically recorded votes. US democracy is based on distrusting the accumulation of power. Thus checks and balances are built in. Australian Ballot principles place trust in the hands of government to conduct an election, but build in transparency so inspection is facilitated. DRE and Internet voting systems put trust in the hands of vendors, commercial 3rd parties, and software with little transparency. Voter verified audit trails preserve the principle of not trusting any self-interested party and the criteria for a fair election by giving transparency to the voter and the public.

A recent poll surveyed security experts' opinions about e-voting. Sixty percent had a negative opinion of e-voting. Their greatest concerns were system and programming errors followed closely by attempts to influence an election's outcome. In contrast, non-experts were primarily concerned with lowered election turnout due to public distrust of e-voting systems (Machlis 2004). These results show the informed expert assessment of the real threat to these systems. The non-expert concern with lowered election turnout shows what is at stake, loss of public trust and confidence.

Given the prevalence of insider fraud and the role of insiders in IS security breaches, trust without appropriate audits and checks is imprudent. Control activities for reducing the likelihood of fraud in commercial settings include: 1) adequate separation of duties, 2) proper authorization of transactions and actions, 3) adequate documents and records, 4) physical control over assets and records, and 5) independent checks on performance (Albrecht 2003). These generic controls together with similar protections such as those enacted in the gambling industry are essential for ensuring secure voting systems. Although it may seem repugnant to some to compare gambling to democratic elections, both require trust in the fairness of the systems to ensure participation.

There is momentum toward the introduction of e-voting technologies brought on by advances in information technology and events such as the 2000 U.S. presidential voting fiasco. This is leading some to rush into implementing these systems and to complacency that results in underestimating the risks involved. Preimesberger (2004) citing the recently held Michigan democratic primaries pooh-poohs the Pentagon for calling off their experiment that would have allowed military absentee voting over the Internet. He takes as proof of security that there have been no reported problems with the Michigan primary. Unfortunately, many in the public may also mistakenly believe that an event without an adverse security breach proves the security of a system.

There is strong indication that the deployment of e-voting systems will continue. This should not be done at the expense of conducting fair elections. This analysis has shown where of the risks lie. It is instructive that some advocates of Internet voting (Mohen and Glidden 2001) agree that the risks are too great for national elections where the fabric of democracy is at risk. However, they point out that there are a number of smaller elections (e.g. school boards) where participation is scanty and there is less at stake. These would be good potential candidates for experiments in Internet voting.

References

Alberts, Christopher J. and Dorofee, Audrey J. (2003). *Managing Information Security Risks: The OCTAVE*^{SM} *Approach*. Upper Saddle Ridge, NJ: Addison-Wesley.

Albrecht, W. Steve (2003). *Fraud Examination*. Mason, OH: Southwestern.

Brand, Richard and Chardy, Alfonso (2004). Venezuela Owns Stake in Ballots, *Miami Herald*, May 28, 2004.

Cranor, Lorrie Faith (2002). Voting after Florida: No Easy Answers, *Ubiquity*

Delk, Kimberly C. (2001). What Will it Take to Produce Greater American Voter Participation? Does Anyone Really Know? *Loyola Journal of Public Interest Law*,

Dill, D. L., Mercuri, R., Neumann, P. G. and Wallach, D. S. (2003). *Frequently Asked Questions about DRE Voting Machines*, Feb. 2003. http://www.verifiedvoting.org/drefaq.asp.

Hoffman, Lance J. and Cranor, Lorrie (2001). Internet Voting: Will it Spur or Corrupt Democracy? *Communications of the ACM*, **44**, **1**, 69 – 71.

IEEE Voting Equipment Standards Security Task Group (2004). Security and Confidentiality Standards. http://grouper.ieee.org/groups/scc38/1583/p1583_-_tg1_main.htm (accessed 2-20-04)

Jones, Douglas W. (2001). Testimony before the House Committee on Science, Washington DC, May 22, 2001. (The record of the oral testimony at this hearing is House Science Committee publication number 107-20).

Kocher, Paul and Schneier, Bruce (2004). Insider Risks in Elections, *Communications of the ACM*, **47**, **7**, 104.

Kohno, Tadayoshi, Stubblefield, Adam, Rubin, Aviel D., Wallach, Dan S. (2003). Analysis of an Electronic Voting System. To appear in *IEEE Symposium on Security and Privacy* May, 2004. http://avirubin.com/vote.pdf (accessed February 14, 2004)

Libbenga, Jan (2004). Dutch e-voting software goes open source. *The Register*. http://www.theregister.co.uk/2004/06/23/open_source_voting_software/

MacCrimmon, Kenneth R. and Wehrung, Donald A. (1986). *Taking Risks: The Management of Uncertainty*. New York: The Free Press.

Machlis, Sharon (2004). Public, security experts' e-voting views differ sharply, *Computerworld*, http://www.computerworld.com/newsletter/0,4902,95094,00.html?nlid=AM, accessed August 6, 2004.

Mercuri, Rebecca (2002). A Better Ballot Box? *IEEE Spectrum*, **31**, **10**, 46 – 50.

Mohen, Joe, and Glidden, Julia (2001). The Case for Internet Voting. *Communications of the ACM*, **44**, **1**, 72 – 85.

Natale, Jessica M. (2002). Exploring Virtual Legal Presence: The Present and the Promise. *Journal of High Technology Law*

Neumann, Peter G. (2001). Risks to the Public in Computers and Related Systems, *ACM SIGSOFT Software Engineering Notes*, **26**, **1**, 14 – 38.

Phillips, Deborah M. and Von Spakovsky, Hans A. (2001). Gauging the Risks of Internet Elections. *Communications of the ACM*, **44**, **1**, 73 – 85.

Preimesberger, Chris (2004). Commentary: Online voting? Of course it can work. *IT Manager's Journal*. http://software.itmanagersjournal.com/software/04/02/14/0245239.shtml?tid=26&tid=44&tid=69&tid=70 accessed February 16, 2004.

Rohde, David (2004). On New Voting Machine, the Same Old Fraud, *New York Times*, April 27, 2004.

Schade, Linda (2004). Diebold Admits Vote Software Used in Maryland

Primaries Did Not Meet Fed Standards, http://baltimorechronicle.com/080304LindaSchade.shtml (accessed August 5, 2004)

Walker, Michael Odell (2002). "Don't Show Them Where to Click and Vote:" An Assessment of Electioneering Law in the United States as a Consideration in Implementing Internet Voting Regimes. *Kentucky Law Journal*

Zetter, Kim (2004). Diebold May Face Criminal Charges, *Wired News*, http://www.wired.com/news/evote/0,2645,63191,00.html