Malfunction or Misfit: Comparing Requirements, Inputs, and Public Confidence Outcomes of E-Voting in the U.S. and Europe

E. John Sebes, Gregory A. Miller

Open Source Digital Voting Foundation
665 Lytton Ave., Palo Alto, CA, USA
http://osdv.org
{jsebes | gmiller}@osdv.org

Abstract: While European democracies are increasingly adopting e-voting technology – including remote voting via public networks – the e-voting experience in the U.S. has been one of disenchantment. The adoption of e-voting technology and outcomes in public confidence in elections processes and results are at significant variance between the U.S. and Europe. We argue that the causes of this variance are rooted in divergent inputs of political traditions that only loosely define systems requirements. In the case of the U.S., several factors, most notably balkanization of the elections processes, have led to the current situation where e-voting technology is a poor fit for unclear systems requirements that are only now becoming clearly understood. A comparative analysis of European and U.S. experiences is the basis for a solvable problem statement for the U.S. situation, together with a solution approach that is being attempted at present.

1 Introduction

Public confidence in the outcome of the use of digital voting technology (hereinafter referred to as "e-voting") is very different in Europe as compared with the U.S. To take two of a great many examples, Swiss e-voting pilot projects [BB06] showed a dramatic increase in participation, via Web-based remote balloting, of habitual non-voters, while in the U.S. advocacy groups called for a return to non-electronic voting.

This striking difference is not merely a reflection of European technophilia and suspicious American technophobia. To understand what one might call "American e-voting dysfunction" we need to look at the American political tradition and the implicit technical and system requirements in our electoral process. We suggest a developmental model of five parts. Political traditions create often-inconsistent sets of elections process goals that create varying trust models, partially determining election system requirements, that are applied (or misapplied) to defining functional requirements for e-voting.

By comparing the U.S. and Europe in this developmental model, we can show how American e-voting dysfunction is as much a result of engineering misfit as it is of technical malfunctions–and indeed that the latter is a consequence of the former. This account of the technology misfit provides the framework for an approach to correcting e-voting dysfunction. This approach is a combination of developmental process, trust process, and functional fit. In addition to being a framework for the creation of sound e-voting systems, this combination is specifically designed to enable a public process of restoring voter confidence in e-voting as a beneficial (not merely neutral) component of an elections system.

2 From Political Traditions to Elections Process

Regarding elections and trust, the American political tradition in the 21st century is still very much based on experience in the 19th century, in at least these three regards: vote buying and coercion; polling-place election fraud; and election fraud in canvassing. Each of these concerns is not only a lasting concern in the American political tradition, but also a driver for formulation of present-day goals for election process, trust models, and system requirements for e-voting systems.

Vote buying and coercion are the most notable instances of voter fraud that are enabled by the lack of effective privacy for casting ballots. There are many historically documented forms [Ca05], but one example may suffice for purposes of comparison: the notorious role of the "precinct boss." In the polling place of a politically corrupt precinct dominated by one political party, the role of a precinct boss was to observe each voter's ballots to determine whether the voter voted in accordance with previous direction, and hence was eligible for reward or punishment.

Concerns over vote buying and coercion have historically been the drivers for the election process goal of the combination of privacy and anonymity in the voting process. More recently, these concerns have manifested in two ways concerning vote-by-mail. In one view, moving the balloting process away from the precinct polling place eliminates the opportunity for precinct-based organized, scalable ("wholesale") coercion/bribery. In another view, large-scale mail voting enables coercion/bribery for a sufficiently large number of voters as to cast doubt on election result validity, especially in close elections. The latter appears to be the more prevalent position, though the actual incidence of this type of voter fraud is debated [MC03], particularly in the state of Oregon (state-wide vote by mail). As voluntary vote-by-mail participation in California has risen above 30%, it may be that parts of the American West are demonstrating a *wertewandel*, or mutation of values, concerning the link between privacy and coercion/bribery.

Vote-by-mail also shows a potential *wertewandel* concerning anonymity. Currently, a ballot is anonymous, but it may be enclosed in an envelope that identifies the voter. Identification is required to determine whether the putative voter is entitled to vote. This approach suggests that current voters may trust election officials not to correlate ballots and voters, despite their ability to do so.

Two other aspects of concern are forms of election fraud—one in the polling places (where access to ballots enables the insertion of spurious or fraudulent ballots); and the other as part of the canvassing process, where undesirable ballots are simply not counted. Many examples have been described [AB00] ranging from the canonical "stuffing the ballot box" to accidents in which a block of ballots is mislaid, invalidated, or simply not counted. Suspicions of fraud are raised when historical voting patterns indicate that the missing ballots could be expected to trend against the desire of elections officials.

These concerns essentially describe a lack of trust in elections officials and in the elected office-holders who have authority or influence over them. Perhaps the most notorious recent incident was in the Florida 2000 American Presidential race. Personal and partisan relationships among the Secretary of State (who had oversight of the elections), the Governor of the State, and the ultimate race winner (the Governor's brother) permanently clouded election results. Although this and similar experiences sparked some excellent work on recommended election reforms [Ca02, Cr04], to date little work has been done to look at how e-voting technology can be trusted to support any of the suggested reforms.

2.1 Election Fraud and the Push to Automation

Election automation is perhaps the most striking and uniquely American result from a political tradition of high sensitivity to election fraud. In the late 19th century, states began using electro-mechanical voting machines that led to the lever machines that remained in wide use in some states as late as 2007. The main driver for adoption was the idea that the machines were more trustworthy by virtue of being less easily manipulated by elections officials to perform wholesale election fraud. This type of automation retained a great deal of public trust despite defects of low auditability, no ballot of reference, no paper trail, etc.

European countries certainly also have histories of election fraud, and real concern over how to structure elections to control it. However, the US may be unique in the degree of mistrust that creates a preference for automation over "pure manual" elections of hard-marked, hand-counted paper ballots.

2.2 Comparison of Election Goals

The elements of American political tradition drive a number of goals for elections processes: privacy of balloting; anonymity of balloting; minimization of distrust in both elected officials and elections officials; auditing and transparency of canvassing and other actions of elections officials. These goals in turn serve as drivers for trust models and systems requirements for e-voting. These goals – and how they define elections processes and technology – exist in marked contrast between the U.S. and many European countries, especially those that make greater use of e-voting. There are two distinct types of contrast: hearty adopters, and non-adopters of e-voting.

In the hearty adopter category are Estonia and parts of Switzerland. Many Swiss cantons have been encouraging vote-by-mail for some time in order to increase voter participation. Although, as noted above, vote-by-mail can create some concerns about anonymity and distrust of elections officials, neither of these values is as strongly held in the Swiss political tradition. Indeed, historically, non-anonymous town-square voting, e.g., a show of hands, was viewed as a traditional value for high-confidence elections.

Similarly, the anonymity concern over vote-by-mail seems largely absent, particularly with the extension to "Internet voting." The high rate of participation in pilots, especially among habitual non-voters, shows a significant trust in elections officials' proper use and dissemination of e-voting data. Anecdotal evidence from elections officials indicates pilot participants were not concerned about privacy, or at least correlation of voter identification and ballot. Participants in the pilot similarly trusted the technology involved, including the PCs, Web browsers, Web applications, the public Internet for communications, and Web application security standards for communication security. A similar set of values is indicated in the Estonian Internet voting experience, with the addition of increased reliance on technology for voting authentication and authorization.

In the non-adopter category are the Netherlands and Ireland. The Netherlands is notable for having effectively outlawed e-voting after nationwide adoption approached 100% in March 2006, with the vast majority of municipalities using the same election system. Shortly thereafter, a documented security issue of the system (described in [Gh07]) and public activism resulted in two government commission studies, the first of which reported that many safeguards thought to be essential to verifiable elections had been ignored because the new technology was not properly understood. The second commission's report suggested the possible future use of open source systems for marking and counting paper ballots. The Dutch government acted to revoke its previous legal framework [Ne07] for defining voting machines for use in the Netherlands; subsequent elections have returned to manually counted paper ballots.

Ireland also conducts elections using manually counted paper ballots. The use of e-voting was seriously considered at one time, however. The Irish government created a Commission on Electronic Voting, which reported in 2004 that it could not recommend the use of an electronic system [Ce04]. Later work also failed to provide the basis for e-voting usage in Ireland, and the commission was dissolved in 2006. There seemed to be a lack of sufficient benefit for the cost and risk of e-voting. Although mitigation of electoral fraud was a potential benefit, it should by no means be taken as an indication of Irish indifference to the issue. Rather, Ireland's rather infrequent (5 and 7 year terms mean that 2 years or more can go by between elections) and simple (often one measure and rarely more than five, each separately balloted) elections are subject to the structured process of manual counting with observation by the general public, and political party officials observing to perform independent counting. The structure and the avid observation may be related in part to the non-trivial method of tallying with Ireland's form of the single transferable ballot.

By contrast, the American response to election fraud concerns has included the use of automation. While the particularly weighty American history (a political tradition of voter fraud, election fraud, corrupt elected officials and elections officials, often referred to *in toto* as "machine politics") of fraud may be one factor, the much higher complexity and frequency of elections may contribute as well.

2.3 Election Complexity and the Push to Automation

American election officials may well look with envy on feasibly hand-counted single-contest ballots, with feasible public visibility of counting – even if they are proponents of e-voting. Election complexity arises partly from a more complex governmental structure than many European countries, resulting in more frequent elections with more contests. Yet some European countries have a similar degree of complexity of offices, and have not adopted e-voting – France is perhaps the best example.

Another fact in election complexity is the result of another form of balkanization, coupled with response to another legacy of American "machine politics" – cronyism, nepotism, patronage, and similar ways in which elected officials use their power of appointing government officials, for their own personal gain. This part of the American political tradition has led to a frequent practice of electing officials that in other times or in other jurisdictions were appointed. The balkanization effect arises from the fact that these locally elected offices are for jurisdictions that are not co-extensive with legislative or local jurisdictions. For example, some parts of a county will be in one school district or another; of the parts that are in one school district, one subset will be in a different water district. A not infrequent result is that in some counties, almost every voting place has a distinct ballot with a distinct set of contests. One anecdotal example: by the time the next President of the U.S. is elected, one author will have voted 4 times in 367 days for a total number of contests numbering at least 30 and likely over 40, in jurisdictions that include: multiple county offices and referenda, offices or referenda from at least 3 local jurisdictions (fire district, harbour district, coastal commission), state and federal offices, and all in a "light year" in which municipal offices, state executive officials, and federal senators are not up for election.

In short, a history of fraud has led to a desire to use automation to mitigate the vulnerability of pure manual paper-based elections, while a history of fraud and patronage has led to a high degree of complexity which elections officials are motivated to manage with automation. Pressure from both sides has encouraged automation in the U.S. for over a century, while public trust in the process has eroded in the more recent past. These two trends may help explain why the American election system is problematic regardless of automation, and in a way that drives automation without trust or even a central or consensual model for trust.

3 From Elections Process Goals to Trust Models

Derived from American political traditions, elections process goals in turn drive trust models for elections and for the reflection of them in a digital voting system. To properly understand e-voting trust models, two aspects of the previous statement are critical: the idea of plural models of trust, and a trend toward trust minimization.

First, the plurality of trust models is derived from a fundamental and critical aspect of U.S. elections systems–an aspect which might be called "balkanization." That is, the U.S. Federal government delegates to states the responsibility for Federal elections. States delegate to county elections officials. Each county, therefore, represents a distinct elections body, making its own choices about election processes, with distinct but (typically) limited regulations or guidance from the state. Each state also makes its own elections laws and regulations within a minimal set of Federal requirements. Not only is there no central or standard regulation or guidance on how to conduct elections (and hence what trust properties an elections process should have), the number of variants is at least two orders of magnitude (dozens of counties in many of the 50 states) larger than in European countries with devolved Federal elections, e.g., Switzerland and France. At the far end of the spectrum are unitary democracies in which the central government regulates how municipalities conduct elections, and most contests are for either one level of local government, or for one legislative representative. In the Netherlands for example, it is not uncommon for an election to consist of just one contest.

We would also argue that current U.S. elections are conducted with a distinct default of mistrust, or at least a goal of minimizing trust and increasing transparency and public auditability. The trend seems to be increasingly in this direction, not only in the realm of public advocacy (particularly in the area of verifiable voting) and public opinion, but also of elected officials. For example, California's Humboldt County is one of the counties in which the chief elections official is pursuing transparency by developing a system for capturing electronic images of all ballots and electronically publishing the set of images. At the state level, again in California, the office of the Secretary of State (regulating county elections officials' activity) recently issued a set of guidelines for polling place physical security practices and for an auditable chain of custody of constrained data items items–such as paper ballots and magnetic media–that record electronically cast ballots. Vigorously pursuing these guidelines, only three counties received cognizance of full compliance–and hence the full ability to utilize e-voting in the February 2008 election.

A third factor is complexity of government structure and oversight over elections. In the US, there is often a variety of partisan elected officials (at the local, county, and state levels) who can influence the way an election is conducted. Not only can election integrity appear to be affected by partisan officials, there is a sometimes complex array of such officials. Further compounding the complexity is that in cases of legal dispute, judicial officials may be notably publicly partisan, or may be elected judicial officials who may be seen as not neutral on issues of the election process. Of course, partisan politics also affects public trust in European elections as well. However, in the US, this trust factor is exacerbated by complexity and is combined with the other factors above.

These three characteristics contribute to the lack of a coherent model of trust in our elections process. A model of trust must consider what roles and operations are trusted with what constraints (e.g., in pursuit of anonymity), and associated controls and logging for auditability. Lacking a definitive trust model for an elections process, it is nearly impossible to derive the basis for trust in e-voting systems–systems that automate parts of the existing election process, much less systems that require modification of the existing process. This lack is greatly exacerbated by the range of trust attitudes, e.g., Oregon and California vs. states that attempt to regulate absentee voting.

3.1 Comparison of Elections Process Goals and Trust

European countries are certainly not uniform in centralization of elections functions or regulations over those functions, not even the countries making more extensive use of e-voting. However, some European voting jurisdictions–for example, the country of Estonia [MM05], or the Swiss cantons that implemented Internet-enabled remote voting–have been clear enough about the elections process and trust to be able to implement aggressive (by U.S. standards) e-voting systems with clear technical requirements. The key differentiator (by contrast with the U.S.) is the active role of the voting authorities (national or cantonal) in the implementation of remote voting.

A different contrast to the U.S. is offered by countries that have explicitly rejected e-voting. Irish experience (in selecting, acquiring, piloting, and studying an e-voting system) was driven by the central government empowered to set goals and empanel commissions to assess a system with respect to those goals. The Dutch experience was even more specific, with the central government creating specific regulations defining voting technology for use by municipalities. When it became apparent that the main e-voting system in use did not conform to regulations, and in addition had serious defects out of scope of the regulations, the Dutch government was empowered to retract the regulation (effectively barring e-voting) and empanel studies to recommend policies to be decided by the central government to regulate the entire country.

Both these types of experience could be said to be a successful outcome with e-voting, in that it became clear whether or not available e-voting technology met the goals for its use. The U.S., by contrast, has no such uniform outcome, or indeed any outcome that is stable for multiple election cycles. Unlike the hearty adopters, county elections offices and the offices of Secretaries of State have had low to no direct involvement in the implementation of e-voting systems and the processes that they automate. Rather, these many, many governmental organizations have acted in the role of a traditional consumer of packaged technology, selecting from a few vendors those systems that seemed to best meet state or local needs. One measure of the lack of positive outcome of this approach is the result of the review, performed for the Office of the Secretary of State of California, of all the polling-place and/or canvassing e-voting systems that had previously been certified by the Office for use in California. Reviewed systems were all de-certified, and only three systems re-certified for limited use for accessibility, with a proviso requiring significantly improved physical and procedural security methods and auditing [So03].

Although the grounds for rejection were mainly based on system security and information security considerations, the overarching question is how these systems came to be used in the first place. Further, how is it that in European experiences the systems used were deemed fit to meet their requirements for use, or specifically unfit? We hypothesize that the European experience was more successful because of the existence of a central body which had authority to define or review proposed requirements, the authority and ability to correlate product requirements with trust requirements; the ability to work with technology vendors to obtain e-voting systems that putatively [a] fit the trust model; and b] are a reasonably close fit to overall systems requirements; and the ability and authority to assess and decide whether systems were in fact fit for use in specific terms.

This combination may have enabled either a definitive rejection of e-voting, o a more multilateral and deliberate process of design, implementation and deployment ([Bo06] describes another such example) than is the typical experience in a U.S. county elections office.

4 From Trust Model(s) to E-Voting Requirements

Whether the above conjecture is valid or not, the facts of life in U.S. elections today are that at present no U.S. county or state will be in as advantageous a position as that we conjecture for some European elections bodies. Balkanization, combined with the packaged product model, have created misfit systems, and have not created a profit motive or market incentive for current or new vendors to create revised or new proprietary products that are a better fit. One overarching reason is the number of jurisdictions; it's not feasible for vendors to obtain, let alone satisfy with products, a set of system requirements that meets the needs – including trust – of even a majority of the jurisdictions. Conversely, elections officials in many jurisdictions are oriented to "making due" with available technology under state or Federal deadlines rather than defining requirements and finding systems that fit them.

Given this situation, the misfit of current U.S. e-voting systems is hardly surprising, and certainly not the result of any lack of effort on the part of the vendors. Given no coherent set of goals, let alone requirements, and no model for how the e-voting systems could be trusted, the vendors had little scope for excellence of fit.

Furthermore, the time-to-market motive–particularly for a fixed set of funds allocated to states by the Federal government's HAVA act [Ha02] –resulted in systems where the misfit resulted in visible malfunction, perceived unreliability, or difficulty of administering, and a growing suspicion about security and integrity. The result has been a general decrease in public confidence.

4.1 Comparison of Trust and E-Voting Requirements

As noted above, the more successful efforts in European e-voting have involved systems that were not off-the-shelf devices, but rather systems developed via bespoke systems integration with a significant degree of stated requirements and a trust model that if not explicit, can be derived for the resulting system and the public confidence outcome of using it.

By contrast, the complex and sometimes historically ugly American political tradition has resulted in a large number of jurisdictions that share, to a varying extent, a particular distrust in elections processes and officials, or at least a dominant pessimism about their integrity, combined with a desire for transparency and verifiability. As a result, American e-voting systems are rather a paradox in that the electorate is implicitly expected to trust computers to partially automate elections processes that are themselves not trusted. At the outset, this is a marginally tenable expectation given most voters' less-than-happy experiences with the reliability, integrity, and security of the personal computers they use. Tenability is strained more with the addition of press coverage of voting device insecurity and election technical snafus.

4.2 Approach to Technical Development Towards Public Confidence

At first inspection, the current situation in the U.S., and the comparison with more positive European outcomes of voter experience and public confidence–not only in similar polling-place e-voting scenarios but also in more aggressive remote e-voting– seems unhopeful for marked improvement.

However, the developmental model, and the approach to development within it, suggests that improvement is possible. We do expect initially to develop e-voting systems requirements to match a coherent trust model or set of elections systems goals. Instead, we use a trust framework rather than a single model, and initially develop requirements bottom up from existing elections processes and the non-misfit functionality of existing e-voting systems. The resulting approach is based on three tenets:

1.   Despite the lack of a single trust model or a central authority with the means to even vaguely define one, it is possible to create a trust framework that enables both a public process of determining whether specific e-voting systems are trustworthy, as well as a systems development process that can be performed with this trust framework in mind.

2.   Existing e-voting systems, in conjunction with a trust framework, can form the basis for deriving election system requirements and functional requirements for specific e-voting devices – especially polling-place devices that are the focus of most of the controversy that strains public confidence.

3. This process and framework require no small efforts to achieve, and the effort is not in the economic interests of vendors or the current operational scope of Federal entities – though some efforts in the latter area may be helpful. However, if the efforts were carried out strictly in pursuit of the public good, and were successful in creating relevant results, then these results could be suitable for adoption and extension by creators of e-voting systems and by Federal and state government organizations with responsibility for elections.

The remainder of this paper describes the trust framework, the method of creating requirements, and the plan for proof-of-concept activities being undertaken by the Open Source Digital Voting Foundation (hereinafter "OSDV").

5 "Trust Framework" Defined

The OSDV approach defines a trust framework in a way that is fairly conventional for high assurance dedicated systems, such as aerospace systems, military systems, and other high-integrity or high-security systems that are fixed-function, dedicated or embedded systems. We observe that many types of e-voting systems (including, but not limited to polling place devices) are or should be fixed function systems that could be trustworthy.

The foundational definition is that a trustworthy device or system does all and only what it is designed to do. A trust framework enables assurance that a particular system is in fact trustworthy. For any particular system, the goal of a trust framework is to be specific about the functions a system is supposed to perform, and how that system could be independently assessed as performing only and all of those functions. The elements of a trust framework are:

Specifications: specific, prescriptive written documentation that defines a particular system and its functions. An implementation of such a specification could be trustworthy if it could be assessed as being conformant to the specification, performing all and only the functions in the specification. As an example of a high-assurance system specification, some Common Criteria Protection Profiles could be considered a specification in this sense. Some U.S. military system "Concept of Operations" documents are good examples of documents that capture a portion of what constitutes a high-assurance specification.

Reference Implementations: a set of hardware and software that implements the specification or a documented subset of the specification, typically with expediency taking priority over other commercially relevant properties. Rapid prototypes of a reference implementation can help to clarify the specification. Even partially complete reference implementations can provide a working example of a trustworthy system, both for proof-of-concept and illustration for others' work on a complete system.

Assessment Guidelines: documentation that specifically describes a methodology for evaluating an implementation of a particular specification. The process of independent assessment is used to evaluate whether a given implementation meets the specification and satisfies other aspects of high assurance, such as software quality. Assessment guidelines are required to enable consistency of assessment efforts across multiple assessments of a system type, and across the efforts of multiple assessors.

Open Assessment Work Examples: Documentation of methods used, findings, results, and overall judgment supported thereby, as a result of the efforts of a complete assessment. System assurance assessments can only assist in building trust and public confidence if the process is transparent and the results are publicly available and vetted. Worked examples of assessment efforts and findings, even undertaken on partial reference implementations, can have a beneficial effect on the clarity of guidelines documents, and serve as a proof-of-concept of the level of effort and feasibility of assessment of a particular specification using corresponding guidelines.

The OSDV approach is to apply this traditional trusted systems approach with related high-assurance systems methodologies to the specifications, reference implementations, open assessments, and documentation of methodologies for e-voting systems. Existing products can serve as the basis for the functional descriptions that are components of a specification for existing product types.

Such efforts have begun on a common system platform for a variety of types of e-voting systems. Platform efforts will be validated in a parallel project to develop e-voting systems based on it, starting with a ballot-scanning device. These efforts are initially focused on polling place devices –as these have caused the most publicly visible effects on voter confidence–but are not intended to be limited to them.

6 The Future: Feasible Development and Assessment of Trustworthy Systems

Assuming that the above efforts are fruitful as envisioned, how might the efforts and results have a markedly positive impact on the current American e-voting dysfunction? One major impact would be to enable a transparently refereed and government supervised evaluation process, similar in some ways to both Common Criteria evaluations performed by today's CCTLs, and to the voting system assessments currently performed for vendors by 3rd parties, in a new program operated by the U.S. National Institute for Standards & Technology (NIST) at the behest of the U.S. Elections Assistance Commission (EAC) [Ea07]. The former types of efforts are standards-based, but intentionally broad and can be burdensome and expensive. The latter are specific to e-voting, but lack public visibility, and cannot be shown to produce consistent results because there are no documented, commonly used (or de-facto standard) system specifications or assessment methods. The OSDV approach will produce results that can fill those gaps in some significant measure.

It is conceivable that in the future, states' certification efforts could be based on the results of transparent, independent evaluations that are feasible and consistent as a result of using standard system specifications and assessment guidelines, together with assessment findings reviews. These standards would be based on OSDV work product, which would have been already proven as usable by other OSDV results in reference implementation, worked example assessment, and public demonstrations. Certainly, the appropriate standards bodies could develop similar standards, but the authors hope the OSDV can fairly quickly develop and validate its work with rapid prototyping and parallel development. The authors envision the OSDV results to be usable during a standards process that would be much shorter as based on the OSDV results than starting afresh with standards committees. We also expect the OSDV results to be complementary to (or in some cases re-use or incorporate by reference) the results of existing work, most notably the U.S. EAC VVSG [Tg07] and work in the U.S. ACCURATE Project [Ac07].

Toward this future, the OSDV Foundation plans to have its reference implementations undergo third party assessment, as well as state certification. Leveraging these results, the OSDV technology transfer plan includes a monetary motivation for others (commercial or public entities) to adopt OSDV technology as the basis for future products: the use of existing, already evaluated platform and core application functionality. This type of adoption could enable product assessments that focus only on extensions outside of the evaluated platform, and be performed more rapidly and cheaply than evaluations of entire systems or revisions to entire systems.

7 The Present: A Digital Public Works Project

Given that vision of future impact, we can describe the current work of the OSDV Foundation as being similar to public works projects and having the following characteristics: based on requirements gathered from existing elections processes; starting from a "blank slate" of functional and trust requirements, without the need to be based on any existing e-voting system; developed transparently in the public eye for the public good, without the motives of commercial gain; performing specification, documentation, prototyping, and assessment efforts in parallel with feedback among these efforts; producing results with proof-of-concept and working examples to validate results. Based on the characteristics, the goal is to deliver proof-of-concepts systems that are developed and documented to be clear about (a) supporting, enabling, and not detracting from election systems requirements discussed above; and (b) the extent and limits of trust required and assumed in the operational environment.

Given these characteristics, we expect OSDV results to provide for the development of systems that could demonstrably support multiple combinations of election system requirements, as well as some well-defined models of trust allocated between technology, practices, physical security, audit, etc.

8 Summary

By comparing European and American experiences, we have argued that current e-voting dysfunction in the U.S. is not based primarily on the use of systems that malfunction due to poor quality, but rather from using commodity systems that are the result of a sometimes hasty and sometimes nearly requirements-free process of development and deployment. Such systems are misfit for their usage and environment because they fail to meet some unstated trust and integrity requirements that might have been derived from a coherent set of trust model and elections process goals–if such a set existed. In the U.S., however, there is no single trust model or single set of explicit (regulatory and legal) requirements, or implicit (operational and design) requirements, but rather a plethora of them. As a result, experience with misfit e-voting technology has drained U.S. public confidence in elections, and created an untenable situation with respect to trust of integrity in e-voting systems.

We have described a partly abductive approach in which we derive system and trust requirements and developmental methodology, by reasoning backwards from both fitting and mis-fitting characteristics of current e-voting devices. We have related this approach to existing misfits, malfunctions, and press coverage that have raised an already high bar in the U.S. (compared with Europe) for trust in elections processes and automation of them. We have described a trust framework and high assurance development methodology that is intended to meet that high bar of trust, and provided a potential model for adoption of OSDV work in that framework.

The overarching goal for adoption is enabling increased U.S. public confidence in e-voting technology and elections in jurisdictions that choose to use high-assurance trustworthy e-voting technology. These intended results will not necessarily be an immediate fit for the needs of a large number of U.S. jurisdictions. However, OSDV results can provide a concrete basis for credible claims of trustworthy systems (a milestone in e-voting in itself), and for iteration of functional requirements to meet specific jurisdictional needs. In addition, the basis for iteration, combined with explicit functional and trust requirements, could further enable some convergence of requirements in multiple jurisdictions, mitigating some effects of the large number of U.S. counties and states.

References

[AB00]   Glenn C. Altschuler and Stuart M. Blumin, Rude Republic: Americans and their Politics in the Nineteenth Century, (Princeton: Princeton University Press, 2000).
[Ac07]   2007 Annual Report, ACCURATE: A Center for Correct Usable Reliable Auditable and Transparent Elections, 21 January 2008, http://accurate-voting.org/wp content/uploads/2008/01/2007.annual.report.pdf
[BB06]   Dr. Nadja Braun, Daniel Brändli, Swiss E-Voting Pilot Projects: Evaluation, Analysis and How to Proceed, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).

[Bo06]   Carol Boughton, Maintaining Democratic Values in e-Voting with eVACS®, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).

[Ca02]   Jimmy Carter, Gerald R. Ford, Lloyd N. Cutler, Robert H. Michel, To Assure Pride and Confidence in the Electoral Process, Report of the National Commission on Federal Election Reform, (Brookings Institution Press, Washington, D.C., 2002).

[Ca05]   Tracy Campbell, Deliver the Vote: a History of Election Fraud, an American Political Tradition – 1724-2004 (New York: Carroll & Graf, 2005).

[Ce04]   Commission on Electronic Voting, "Interim Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System", March 2006.

[Cr04]   Ann N. Crigler, Marion R. Just, Edward J. McCaffery, Rethinking the Vote: The Politics and Prospects of American Election Reform, (Oxford University Press, 2004).

[Ea07]   United States Election Assistance Commission, EAC Receives Lab Recommendations from NIST, (Press Release 18 January 2007). http://www.eac.gov/ News/press/docs/01-18-07-eac-receives-lab-recommendations-from-nist

[GH07]   Rop Gonggrijp and Willem-Jan Hengeveld "Studying the Nedap/Groenendaal ES3B voting computer a computer security perspective" 2007 USENIX/ACCURATE Electronic Voting Technology Workshop, Boston, USA.

[Ha02]   Help America Vote Act of 2002, United States Public Law 107-252, 107th Congress, http://www.fec.gov/hava/law_ext.txt

[MC03]   Lorraine C. Minnite, David Callahan, Securing the Vote: An Analysis of Election Fraud, (New York: Demos, A Network for Ideas and Action, 2003).

[MM05]   Ülle Madise, Tarvi Martens, E-Voting in Estonia 2005: The First Practice of Country-Wide Binding Internet Voting in the World, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).

[Ne07]   Intrekking Regeling voorwaarden en goedkeuring stemmachines 1997, Uit: Staatscourant 19 oktober 2007, nr. 203 / page 10.

[So03]   Office of the Secretary of State of California, Secretary of State Debra Bowen Moves to Strengthen Voter Confidence in Election Security Following Top-to-Bottom Review of Voting Systems, (Press Release 3 August 2003). http:// sos.ca.gov/ elections/ voting_systems/ttbr/db07_042_ttbr_system_decisions_release.pdf

[Tg07]   Technical Guidelines Development Committee, Voluntary Voting System Guidelines, Draft, (United States Election Assistance Commission, 09/06/2007).