Preliminary Analysis for Securing Vote Capture and Verification in DV and IV Voting Systems

Draft Version March 2, 2005

4 March 2005

National Institute of Standards and Technology (NIST)

Provided for consideration by the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission under the requirements of the Help America Vote Act (HAVA) of 2002.

Preliminary Analysis for Securing Vote Capture and Verification in DV and IV Voting Systems Draft Version

March 2, 2005

John Kelsey

Authority This document has been provided for consideration by the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission under the requirements of the Help America Vote Act (HAVA) of 2002.

Disclaimer This document is a work in progress, provided solely as draft input to the TGDC. Portions of this document may change substantially.

1 Introduction

Based on HAVA requirements, voting systems must provide a step during the voting process in which the voter can review and verify his choices. This step allows the voter to notice and correct errors, and decreases the impact of a confusing ballot design or other problems during the process of capturing the voter's choices. This note discusses the NIST voting team's current thinking on how this voter verification step can be used to secure future voting systems, inlight of the issues raised by TGDC resolution 12-05.

1.1 The Importance of the Verification Step

Voting system security relies on correctly carrying out many steps--correctly setting up the machines, loading the ballots, accurately recording the choices intended by the voter, storing those choices securely, transferring them to some central facility, and finally, counting and auditing them. However, securing the process of capturing and verifying the voter's choices is complicated by the need for voter privacy. Most other steps can be done in a way that is carefully audited, closely observed by many people, or rerun on different machines by different people in case of error or dispute. All these levels of auditing and observation make many attacks which are theoretically possible against a voting system quite difficult in practice, at least if good procedures are followed by election officials.

The process of capturing from the voter his intended choices is different. Voting is done in private; the voter cannot be given a receipt which allows him to demonstrate how he voted, election officials can't observe his vote and then verify that the system recorded it correctly, and the voter can't easily be called back to the polls to vote the same way a second time. The only person who can determine whether the voter's intentions were correctly captured is the voter, and the vote verification step required by HAVA can be used by a voting system to produce evidence by which the contents of the voter's clearly-indicated choices can be audited in a meaningful way, without sacrificing the secrecy of the vote.

In order to audit the process of capturing the voter's choices, the voting system needs to produce two records of those choices, each with independent validity. That is, an attacker who can compromise one of these records should still face a difficult task in compromising the other. The rest of the voting system can then compare these records and verify their correspondence as part of the normal process of collecting together and counting votes. One record is created and stored as a result of the process of capturing the voter's choices; another record is created and stored as a result of the voter's verification of those choices. This can be done with voting systems which produce a voter-verified paper audit trail (VVPAT in the rest of this document), or with all-electronic voting systems which use separate hardware and software to capture the voter's choices and verification, and to store the results. Voting systems that do so will be called "dual-verification voting systems" in the rest of this note. As discussed below, the issues raised by resolution 12-05 can best be addressed in the context of dual-verification voting systems.

The NIST voting team currently plans to draft standards which will:

a. Require than future electronic voting systems be designed to produce two distinct records of independent validity during the process of gathering votes, one from the process of capturing the voter's choices, the other from the process of having the voter verify those choices, regardless of whether these systems are in DV or IV. This will make them dual-verification systems.

b. Specify requirements for producing and maintaining these separate records in a way that supports their use in auditing the underlying process of accurately capturing clear indications of the voter's choices. This differs considerably between DV and IV systems, and is addressed in a preliminary way below.

c. Specify how these separate records shall be used to audit the interaction between the voting system and the voter, without sacrificing voter privacy. This is mostly addressed in the note on multiple representations.

1.2 Resolution 12-05 and the DV/IV distinction

The form of the separate records produced by the process of capturing voter selections (called "capture" in the rest of this note) and the process of having the voter verify his selections (called "verification" in the rest of this note) determines whether a voting system falls into the class of DV or IV systems. A DV (Directly Verifiable) voting system allows the voter to verify at least one representation of his votes with his own senses, not using any software or hardware intermediary that might be compromised to mislead him, which is then used in the normal vote counting process. An IV (Indirectly Verifiable) voting system uses some hardware or software intermediary to allow the voter to verify all representations of his choices.

The text of the resolution is as follows:

> The TGDC has considered the various means by which a voting system allows a voter to verify that his or her vote was captured as the indication of the voter's choice. All voting systems must provide such means, as stated in HAVA 2002 section 301(a)(1)(A)(i). Such voter verification means can be categorized as either "direct," as with optical scan or a machine-generated paper ballot, where the voter can directly examine the representation of his ballot, or "indirect," as with many touch-screen Direct Recording Electronic-- DRE machines, where the voter can only verify the "fundamental representation" of his ballot through the assistance of intervening hardware and/or software.
>
> For voting systems that create more than one representation of the voter's ballot (such as one electronic and one on paper), the TGDC interprets the HAVA language to require that such voter verification must apply to the representation

> (to be called here the fundamental representation) that is used for the initial vote tabulation.
>
> The TGDC therefore finds it useful to divide voting systems into two categories: those (class DV) where each voter is presented a fundamental representation of his ballot that the voter may directly verify, and those (class IV) not in class DV.
>
> The TGDC has concluded that voting systems in class IV or DV must be held to significantly different security requirements, including different constraints on voting system development, different requirements for system documentation, and different testing to mitigate the different risks associated with each type of voting system.
>
> The TGDC therefore requests that NIST perform research and develop standards documents that:
>
> 1. Clarifies the distinction between class DV and class IV voting systems as may be necessary,
>
> 2. Elaborates and defines the different requirements to be satisfied by class DV and IV voting systems, and
>
> 3. Reviews methods of verification accessible by voters with disabilities.

The most important point to be made about this distinction is that, in security terms, the really important distinction is whether the step in which votes are captured from and verified by the voter is auditable. In a dual-verification architecture, the records from the capture and verify processes have independent validity, and so can be used to check one another. This makes the process of getting votes from the user auditable.

1.3 Verification and the "Fundamental Representation"

Resolution 12-05 raises the concern that the record of his choices which the voter verifies may not be the one initially counted:

> For voting systems that create more than one representation of the voter's ballot (such as one electronic and one on paper), the TGDC interprets the HAVA language to require that such voter verification must apply to the representation (to be called here the fundamental representation) that is used for the initial vote tabulation.

This issue is addressed more fully in the note on multiple representations. To summarize, NIST has concluded that the relevant requirement is not that one representation or the other must be counted first or assumed to always be authoritative. Rather, the requirement is that all representations are checked against one another during the normal counting and auditing procedures of the voting system, so that any substantial

disagreement between the representations is overwhelmingly likely to be caught. (In particular, it is not acceptable to keep one of the representations back to be used only for recounts.)

If these requirements are met, then the NIST voting team concludes that the concern expressed in the resolution has been addressed.

1.4 Summary of Current Thinking on Voter Verification and Security

The following is a high-level summary of the NIST voting team's current thinking on the issues relating to independent verification records and resolution 12-05:

a. Future electronic voting systems shall provide distinct sets of records of independent validity from the processes of capturing and verifying voter choices. This is a requirement to allow the process to be meaningfully audited, and it leads to "dual-verification" architectures.

b. Directly Verifiable (DV) systems produce a record for voter verification which the voter may verify with his own senses, without relying on any hardware or software intermediary. In the context of dual-verification systems, DV systems produce an electronic record of an indication of the voter's choices, whose validity and usefulness in determining the voter's intentions does not depend entirely on the paper record or its integrity.

c. Indirectly Verifiable (IV) systems allow a voter to verify the records produced by his vote only via hardware or software intermediary. In the context of dual-verification systems, IV systems produce two distinct electronic records of an indication of the voter's choices, each of whose validity and usefulness in determining the voter's intentions does not depend on the other record or its integrity.

d. The distinction between DV and IV is important in terms of the specific security requirements necessary to produce meaningfully independent records, and the concerns that arise for the two classes of voting system are often different. However, the underlying security goal (two independent records of the voter's expressed intentions, in order to allow auditing of each record by the other) is the same.

e. The distinction between DV and IV systems is not as clear as it first appears. DV systems typically produce human-readable paper ballots, which are then scanned electronically for efficient processing. Some IV systems using advanced cryptographic techniques provide the voter a paper receipt, but one that only allows verification of the existence of a corresponding electronic record in the final count.

f. Neither class of systems is inherently more secure. In some areas, DV systems have important advantages; in others, IV systems have the advantages. It is possible to design a very secure voting system of either class, and likewise possible to design a very insecure voting system of either class.

g. Dual-verification voting systems produce records of independent validity from the capture and verify processes of interacting with the voter. These systems provide an important security improvement over systems without such distinct sets of records. However, they can do nothing by themselves to secure the other parts of the voting system. In particular, the creation of these distinct records does nothing to guarantee that they're actually counted, aren't tampered with on the way to the central counting facility, etc.

h. If either the capture or verify process is compromised by an attacker, that attacker can create genuine confusion between the two records, and may be able to leave the election officials unable to reconstruct the correct votes. (This would not allow an attacker to change the election outcome, but might require re-running the election.) Similarly, either process being compromised is enough to involuntarily violate voter privacy. Some of these issues are discussed in greater detail in the note on multiple represntations.

2 Clarifying the Distinction Between DV and IV Systems

The first part of the resolution defines the distinction between DV and IV systems, and calls upon NIST to address it. Quoting:

> ... The TGDC has considered the various means by which a voting system allows a voter to verify that his or her vote was captured as the indication of the voter's choice. All voting systems must provide such means, as stated in HAVA 2002 section 301(a)(1)(A)(i). Such voter verification means can be categorized as either "direct," as with optical scan or a machine-generated paper ballot, where the voter can directly examine the representation of his ballot, or "indirect," as with many touch-screen Direct Recording Electronic-- DRE machines, where the voter can only verify the "fundamental representation" of his ballot through the assistance of intervening hardware and/or software.

Further, the resolution directs NIST to perform research and draft standards text which:

> 1. Clarifies the distinction between class DV and class IV voting systems as may be necessary,

To a first approximation, DV systems are voting systems which produce a paper record for the voter to verify with his own senses, and which then use that paper record in the initial counting and auditing process. IV systems are voting systems which are not DV systems, but in this note, the voting systems of interest are dual-verification voting systems.

Expanding on this, a DV system is one in which the voter verification step is done without any reliance on the accuracy of hardware or software. This means that the integrity of this step, and the records it produces, are independent of the integrity of the hardware and software used to capture voter choices. The class of IV systems is much

broader, encompassing systems built on the "frog protocol" from the MIT/Caltech report, cryptographic voting systems, and many others.

2.1 Directly Verifiable

Directly Verifiable (DV) systems produce at least one independent record which the voter can verify directly with his senses, and which is used in the initial count either directly or in an auditing step, as discussed in the note on multiple representations. In principle, direct verification could be done on many different media; in practice, all current and proposed DV systems of which NIST is aware are based on paper.

2.1.1 Examples

Examples of DV Systems which produce independent records from both the voter's selections and his verification of those selections include:

a. A DRE with a voter-verified paper audit trail (VVPAT).

b. A DRE which produces an optical scan ballot.

In these examples, the system is in DV (and would be acceptable in the standards contemplated by the NIST voting team at present) only if both the electronic and paper records are used in the initial count. This use can be direct counting, or indirect through some auditing step that will catch any substantial number of insertions, deletions, or alterations of either the electronic or paper records with very high probability. The NIST voting team intends to explicitly exclude VVPAT systems whose paper audit records are not examined except in case of a recount from future standards. A more complete discussion of these issues appears in the multiple representations note.

2.2 Indirectly Verifiable

Indirectly Verifiable (IV) systems allow the voter to verify his selections indirectly, through the use of some hardware and software which presents a summary of his choices to him. This allows the representations of the voter's choices to remain in entirely electronic form. NIST currently plans to draft standards which require that this verification take place in an way which produces distinct records from the capture and verify processes, and which ensures that these records have some independent validity.

2.2.1 Examples

By the definition in Resolution 12-05, any system not in DV is automatically in IV. NIST intends to further exclude from the set of allowable IV system any system that does not provide dual verification.

Some examples of dual-verification IV voting systems include:

a. The "frog" protocol described in the MIT/Caltech report. (A voting machine in this scheme consists of a voting station and a verification station which are kept separate. A voter inserts a memory card into the voting station to make his selections, and then takes the memory card to the verification station to cast his vote.)

b. A DRE with a camera mounted above the screen, which is independent of the DRE, and is triggered by a request from the DRE each time the voter accepts a verification screen. (Additional hardware could be added to capture audio votes for verification, though this raises privacy issues.)

c. Cryptographic voting schemes whose security depends on correctness of proofs, and in which the voter can verify the inclusion of his vote only through a software or hardware intermediary, but the voter gets to choose which intermediary and can write his own.

d. A DRE with an independent device functioning as a terminal screen for verifying the voter's choices, in which the the terminal screen logs everything displayed on it and the voter's indication of acceptance or rejection of the displayed vote summary in a way that is protected from the DRE.

In all these examples, the IV voting system must produce and maintain independent records, and must use both in the normal counting process. The set of possible dual-verification voting systems in IV is much larger and far more diverse than the set in DV, and includes many voting system architectures that don't appear in the examples above.

3 Special Requirements and Concerns for DV Systems

DV systems use paper. A number of special concerns arise with paper-based systems, including reliability of printing equipment (typically much lower than the reliability of all-electronic equipment due to the need for moving parts and consumable stocks of paper and ink), error rates of scanning and counting paper records electronically, the possibility of differences between the human-readable representation of paper audit records and the corresponding scanned-in electronic representation, and the difficulty of randomizing printed paper records inside a ballot box to avoid leaving an ordered record of votes. Some of these will be discussed below, but a more complete summary of issues and near-term requirements may be found in NIST's draft standards for VVPAT systems.

3.1 Requirements

The following are some requirements that apply especially to DV systems.

a. Paper records shall be printed in a way that is machine-readable and human-readable. It is acceptable to have paper records with some parts that are not human-readable, so long as the other requirements are met.

b. Paper records shall be printed in a completely public format. This encompasses both the human- and machine-readable information.

c. When paper records are scanned into electronic form, there are typically some records that aren't scanned correctly due to alignment issues or other problems. However, the probability of any record's electronic version being different than its human readable version as a result of error shall be astronomically small. Error-correcting codes can make this reasonably easy to accomplish.

d. Paper records shall include a unique identifier, which allows linkage of each paper record to its corresponding electronic record. This identifier shall:

(i) Either be guaranteed to be unique, or be unique with overwhelming probability.

(ii) Not be practical for the voter to note down without a camera or other special hardware in the course of verifying his vote. The identifier may be physically hidden from the voter in some way, or encoded in some non-human-readable format.

(iii)Not reveal the order of the votes at any machine, or the precise time at which the vote was cast, or any other identifying information about the voter.

e. Paper records shall not reveal the precise order of voters at a given machine, and should randomize that order to the extent possible.

f. The process of carrying electronic and paper records to the central counting process, and of storing them, shall not leave both sets of records vulnerable to compromise by the same person or small group of people.

3.2 Concerns Not Addressed by Requirements

Some concerns are hard to address by requirements at present, but may be addressed in the future, as the NIST voting team learns more about the special requirements of DV systems. Among these:

Paper records are prone to errors in scanning and to damage during scanning which can make the records quite hard to recover. Standards should address making these paper records as robust as possible, and making the scanning process as thorough as possible. However, relatively high error rates csn seriously complicate auditing procedures.

Paper records for voter verification can be hard to use. This may facilitate a straightforward attack on a DV system, in which the compromised voting machine displays the votes as selected on the screen, but prints them with some desired change, changing the screen representation to match the "error" if the verification doesn't happen fairly quickly.

A consequence of the above attack is that voting systems should keep track of the number of rejected verification attempts each machine has had.

It is much easier to scan paper records on a long roll than paper records printed on hundreds of pieces of paper. However, a very long roll of paper allows an attacker to learn the order of votes at a machine for some period of time. It isn't clear whether some compromise could allow rolls of paper containing relatively small numbers of votes (i.e., 10) without unacceptably compromising voter privacy.

Even when paper records are cut apart, they are likely to settle in approximately the order in which they were printed. It isn't clear how to address this.

Paper records have a much higher likelihood of undetected failures (a printer that either prints hard-to-read things or stops printing altogether) than other records. This makes attacks based on simply replacing a bunch of paper records with blank paper a potential problem.

Additional discussion of near-term requirements for DV system may be found in the draft report on VVPAT voting systems.

4 Special Requirements and Concerns for IV Systems

Some special requirements will apply to IV systems, in order to ensure that the process of capturing the voter's choices and the process of getting a verification from the voter of the summary of his choices yield representations of the voter's choices whose validity is meaningfully independent. The goal is to avoid single points of compromise or failure between the multiple representations. Some of the requirements that result from this requirement are discussed below. These requirements are preliminary, however, and are still being researched and discussed at the writing of this note.

4.1 Requirements

The goal is that the dual-verification IV voting system produce records from the capture and verify process whose validity is independent. This leads to a number of proposed requirements:

a. Any direct communications between the capture and verify processes shall make use of public and fully specified formats. Implementations shall prevent any other communications from taking place between these processes, and shall defend the two processes from hostile communications (such as buffer overruns). Testing shall verify that this is done correctly.

b. The hardware and software producing records from the capture and verify processes shall be independently sourced (not bought from the same company).

c. The hardware and software producing records from the capture and verify processes should use different operating systems and other software whenever possible.

d. The capture and verify processes should communicate only via writing to a removable memory device, so that the memory device can be saved for recounts if necessary.

e. The hardware and software implementing the capture and verify processes shall demonstrate good security against intrusion and escalation of privelege. Testing of the voting system shall verify this.

f. The capture and verify processes shall not share any cryptographic key material used for any other purpose but to communicate with one another.

g. The records stored for both systems shall not reveal the order of votes, individually or taken together.

h. All assistive technology, languages, etc., should be available on both machines, for both processes, when the verification step is taking place on a different machine.

i. The processes of setting up, storing, and loading software and ballots onto hardware used by the two processes shall not leave a single person, device, or holder of a cryptographic key with the authority to compromise both processes.

4.2 Concerns

The major concern that remains with IV systems is deciding how independent the processes of verification and capturing votes are.

Common bugs or vulnerabilities can lead to problems with both records from the same underlying flaw. For example, if the machine used for capturing voter selections and the one used for vote verification are built by the same manufacturer, then it's possible that the same programmer could have inserted a vulnerability in both machines. A more likely scenario is that the same operating system or some common toolkit is used for both machines, leading to both machines having the same security vulnerabilities.

The range of IV systems is enormous. IV systems based on the "frog" or "votamatic" protocols tend to work with underlying electronic records. IV systems based on independently recording images or sounds presented to the voter during voter verification often will work with raw images or sounds, and so will have many of the properties of paper--high error rate during scanning into an electronic form and potential privacy violations for alternative-language voters, for example. Many of the requirements above apply imperfectly to such systems.

A generic attack on almost all voting systems involves introducing differential errors--a vote for John Smith is accidentally misread as a vote for Mary Jones a small fraction of the time, but the voter can correct it in the verification step if he notices it. One

procedural way to make this kind of attack more difficult is to note the number of rejections done by the verification process, and to carefully audit machines which have unusually high numbers of rejections.

5 Accessibility Issues for DV and IV Systems

The resolution directs NIST to draft standards text which:

3. Reviews methods of verification accessible by voters with disabilities.

5.1 IV Systems

Most IV systems can maintain both records in an electronic format. Electronic records can make use of the full range of assistive technology. Other than any additional overhead involved in using multiple devices to cast his vote, a disabled voter need have no more trouble using such an IV system which produces independent records from the vote capture and verification steps than with any other electronic voting system. Similarly, alternative-language ballots are no harder to handle with such IV systems which produce independent records than with any other electronic voting system.

It is possible to design an IV system which captures an image or sound recording of what the voter had presented to him during the vote verification process. Such systems potentially have many of the same set of problems as paper-based systems. In particular, use of assistive technology or alternative-language translations is captured by the independent recording device, potentially costing the voter his privacy, and the lack of the underlying electronic record in the verification process means that assistive technology may bot always be available for voter verification in this kind of scheme.

5.2 DV Systems

DV systems raise some important problems with respect to accessibility for voters who either can't see well enough to read a printed summary of their vote, or who need the summary translated into an alternative language. Electronic records can be presented over headphones, or magnified on a screen to make them accessible to people with impaired vision, or translated into an alternative-language on screen without necessarily violating the privacy of the voter. Paper records are much less flexible, and DV systems are designed with the assumption that the paper records can be verified independently by voters.

There appear to be two reasonable ways to deal with the accessibility issues:

a. Voters who cannot make use of the direct verification process can simply be left to trust the integrity of the vote capturing process.

b. Voters who cannot make use of the direct verification process can be allowed to use an indirect verification process.

The NIST voting team is deeply uncomfortable with the first approach. This is not merely because of a perception of unfairness; there are a number of security problems raised.

In some places, a sizeable fraction of the voters will have trouble verifying the printed ballot summary as required by the DV system. Worse, the voting machine can note the use of assistive technology when deciding whether to alter a voter's choices. (In this case, a corrupt DRE might display the right vote on the screen or play it into the headphones, but write the wrong vote to both electronic memory and the printed ballot.) Such an attack doesn't appear to be preventable in a simple DV system by purely technical means; widespread fraud of this kind can be detected by parallel testing or by some sighted voters using the assistive technology, but also carefully verifying the paper record.

Non-English language voters raise a similar set of problems: for privacy reasons, it may be a bad idea to print the ballot summary for an alternative-language voter (in some polling places, there will be very few alternative-language voters). On the other hand, not printing the ballot in the same language used for making selections surely decreases the chances that the voter will actually check the paper record for correctness.

For all these reasons, a better solution appears to be the provision of at least one voting station that implements an IV voting system consistent with the requirements for IV systems. This system can use the machine-readability requirement of the paper records from the DV system; the voter takes his paper record to a second verification station, feeds it into the reader, and gets a computer-mediated verification step which meets the security requirements for IV systems. Alternatively, it can be an entirely separate IV voting system.

6 The Special Case of Cryptographic Voting Systems

Cryptographic voting systems fall into the class of IV systems by the definitions used in both resolution 12-05 and this note. However, they have a number of unusual properties, which make them fundamentally different from other voting systems in their security requirements, their security properties, and how they must be evaluated.

6.1 Security Requirements

As a rule, cryptographic voting systems are much less dependent for their security on the integrity of computer hardware and software than DV or other IV systems. While any voting machine which is compromised can record votes and thus violate voter privacy, a compromised voting machine in a cryptographic scheme can do very little mischief without an overwhelming probability of getting caught. This has the effect of converting most attacks that attempt to change the outcome of an election into attacks that disrupt the election. (Again, by compromising a voting machine, it is always possible to do this; the voting machine can simply delete all copies of the votes it captured at the end of the day.)

The voter verification step in cryptographic voting schemes ultimately makes use of hardware and software intermediaries; even when a voter is given a printed receipt, the receipt can be shown to have had its vote counted only by carrying out a complex set of calculations.

Where other IV systems rely on the integrity of two independent machines that the election officials of the state or county chose, cryptographic voting schemes allow the voter to choose his own intermediary, and allow him to use as many as he can find. He may even write his own software to do the verification.

On the other hand, the voter's choices are verified by the voter during voting on the machine which also captured those votes; only the receipt given to the voter in a cryptographic scheme is verified independently. If there is anything the voting machine can do to mislead or confuse the voter about what he is verifying, the independent voter verification step later will not catch it. This leads into details of the usability of these systems which are still to be considered.

6.2 Security Properties

Cryptographic voting systems typically provide an additional security property: While IV systems discussed in this note produce two records of the voter's choices which can be used to meaningfully audit one another, additional security mechanisms are needed to ensure that those records are successfully carried to the counting process and are used correctly. Cryptographic voting systems provide an assurance, not only that the correct set of choices was recorded somewhere, but that those choices were included in the count. This makes them fundamentally different from other IV voting systems.

6.3 Evaluation

Open-ended evaluation and testing of voting systems is the subject of another note. However, cryptographic voting systems must be evaluated in a very different way from all other voting systems. Open-ended evaluation of voting systems is generally important because of the insufficiency of simply mandating good security in each piece of a system; a standard can easily demand the use of strong cryptography, good coding practices, and excellent locks and seals, but these pieces can always be put together in weak ways. However, with a DV or non-cryptographic IV system, the nature of the evaluation is relatively straightforward--some capable people study the documentation (particularly the directions given to election officials) and the system's description, and attempt to find weakneses in it. It is understood by all that a perfectly good voting system architecture, such as the frog protocol proposed by the MIT/Caltech report or the VVPAT systems described by many sources in the literature, can be implemented badly--the purpose of the evaluation should be as much to catch and correct bad implementations as bad designs.

With cryptographic voting systems, the most important part of the security is in the cryptographic protocols. These protocols must be evaluated in an open-ended way, but not generally by the same people as a voting system, and not at all in the same way. Verification of proofs and examination of attacks that bypass or invalidate those proofs are both very important in such evaluations, but checklists on locking down commercial operating systems, automated testing for buffer overruns in source code, and similar tools are not especially useful. An entirely different evaluation process needs to take place.

NIST normally standardizes on cryptographic protocols and algorithms by either waiting for widespread acceptance of them in the cryptographic community, or by drawing them from some existing standardization group which has accepted them. At present, it is unclear what existing standardization body would evaluate cryptographic protocols for voting, and how else voting protocols might be certified as acceptable for use. Any such certification would need to have some method for decertification, in case attacks were developed on the protocol, or any of the underlying mathematical assumptions were shown to be false.

7 Conclusions

This note has summarized the NIST voting team's current thinking on the use of the verification step during voting to improve voting system security. Closely related issues are discussed in the note on multiple representations, and many near-term issues relating to DV systems may also be found in the draft VVPAT standard.