Cleveland-Marshall
College of Law Library

Cleveland State University
EngagedScholarship@CSU

Law Faculty Articles and Essays

Faculty Scholarship

8-2009

E-Voting and Forensics: Prying Open the Black Box

Candice Hoke
Cleveland State University, s.hoke@csuohio.edu

Sean Peisert
University of California, Davis and Lawrence Berkeley National Laboratory, peisert@cs.ucdavis.edu

Matt Bishop
University of California - Davis

Mark Graff
Lawrence Livermore National Laboratory

David Jefferson
Lawrence Livermore National Laboratory

Follow this and additional works at: https://engagedscholarship.csuohio.edu/fac_articles

 Part of the Election Law Commons, and the Law and Politics Commons

How does access to this work benefit you? Let us know!

Repository Citation

Hoke, Candice; Peisert, Sean; Bishop, Matt; Graff, Mark; and Jefferson, David, "E-Voting and Forensics: Prying Open the Black Box" (2009). *Law Faculty Articles and Essays*. 830.
https://engagedscholarship.csuohio.edu/fac_articles/830

This Article is brought to you for free and open access by the Faculty Scholarship at EngagedScholarship@CSU. It has been accepted for inclusion in Law Faculty Articles and Essays by an authorized administrator of EngagedScholarship@CSU. For more information, please contact research.services@law.csuohio.edu.

Cleveland State University

From the SelectedWorks of S. Candice Hoke

August, 2009

E-Voting and Forensics: Prying Open the Black Box

Candice Hoke, *Cleveland State University*
Matt Bishop
Mark Graff
Sean Peisert
David Jefferson

Available at: http://works.bepress.com/s_hoke/26/

E-Voting and Forensics: Prying Open the Black Box

Matt Bishop and Sean Peisert
Department of Computer Science
University of California, Davis
{*bishop, peisert*}*@cs.ucdavis.edu*

Candice Hoke
Cleveland-Marshall College of Law
Cleveland State University
candice.hoke@law.csuohio.edu

Mark Graff and David Jefferson
Lawrence Livermore National Laboratory
{*graff5, jefferson6*}*@llnl.gov*

Abstract

Over the past six years, the nation has moved rapidly from punch cards and levers to electronic voting systems. These new systems have occasionally presented election officials with puzzling technical irregularities. The national experience has included unexpected and unexplained incidents in each phase of the election process: preparations, balloting, tabulation, and reporting results. Quick technical or managerial assessment can often identify the cause of the problem, leading to a simple and effective solution. But other times, the cause and scope of anomalies cannot be determined.

In this paper, we describe the application of a model of forensics to the types of technical incidents that arise in computer-based voting technologies. We describe the elements of e-voting that current forensic techniques can address, as well as the need for a more structured analysis, and how this can be achieved given modifications to the design of e-voting systems. We also demonstrate how some concrete forensic techniques can be utilized today by election officials and their agents, to understand voting system events and indicators. We conclude by reviewing best practices for structuring a formal forensics team, and suggest legal steps and contractual provisions to undergird the team's authority and work.

1 Introduction

Election administrators have been required to manage rapid changes in voting technology. Even with ample time, staffing, and technical support, these changes would present tremendous challenges to the most experienced administrators. But these resources are typically not available. And because of incidents such as the alleged multi-year fraud involving e-voting machines in Kentucky [12], these problems can no longer be dismissed as theoretical [22].

This paper considers the problem of *forensic examination* of e-voting systems. These reviews occur after the election, when it has been determined that something went wrong, or may have gone wrong. We place our analysis in the framework of a formal model of forensic analysis, Laocoön [31].[1] Laocoön uses fault graphs based on safety properties and security policies to impose a structure on log data. That structure describes the sequence of steps that take place, and the data that can be used to show that these steps took place. In this paper, we look at voting systems and address the following questions, using the framework of our model:

- What questions can a forensic examination answer?
- When should election administrators consider an election forensic examination?
- How should they prepare for an examination?
- Who should be included on the forensic team?
- What sort of legal, contractual, and practical provisions may be needed?

Equally important is what this paper does *not* do. This paper does not study the merits of e-voting, or of specific types of e-voting systems. It accepts that these systems exist, and are used, and asks what to do should they fail or appear to function anomalously. The paper does not analyze or discuss proposed voting systems (such as Clarkson's [14] or Yee's [39]) because its goal is to discuss election forensics in the *existing* election environment, not in some future environment (although much of the discussion may apply there). Nor does this paper deal with specific auditing techniques [16, 19, 23] because its focus is on *how* and *when* to apply those methodologies and technologies as part of a forensic audit. Auditing techniques may provide an indication that forensic analysis is necessary and may be useful tools within the forensic analysis. However, there are many other indicators that forensic analysis is necessary, and there are many other useful tools within the forensic analysis.

[1] /Lay-ah-co-ahn/; who was the Trojan (an ancient detective of sorts) who recommended not letting the Trojan horse into Troy.

After a discussion of the background, we derive general questions that a forensic audit would consider from the objectives of an election. This leads to specific indicators of possible problems, at a much lower level than the general questions. Given these precise indicators, we can then apply our model of forensics to show what data needs to be collected to enable the forensic audit to succeed, and conversely, what data that is needed cannot be collected due to system limitations.

2 Problem Statement

During an election, an optical scanner may fail to read ballots consistently, or a server may freeze as it tabulates votes. Voting machine memory cards or optical scan ballots may appear to be missing in the canvass report. During every election cycle, experienced election administrators around the nation anticipate and successfully cope with events like these. But sometimes events are not amenable to quick resolution. Vote totals cannot be reconciled, or equipment or software failures recur without explanation. What happened? Are totals accurate and complete? Can election officials in good conscience certify the results of the election before these questions are answered? Will the public accept the results, knowing there are unanswered questions about the votes? Should candidates demand a recount?

The technical explanations needed to answer such questions lie in the realm of *election forensics*: the process of analyzing and discovering the causes and cures of technical problems that might have an impact on the validity of the results. If the problems involve computers, then computer forensics are likely a large part of the expertise required.

The forensic specialists can be asked to determine the cause of unexpected computer behavior, whether the vote totals were affected, and to recover missing or damaged voting records. They can also provide technical evidence about the integrity of the voting data.

In this paper, an *e-voting system* is simply a computer-based mechanism for conducting part of an election. It includes DREs with and without voter-verified paper audit trails, opti-scan systems, election management systems, and others. The forensic models and framework is similar for all such systems. However, the specific manner in which the framework is applied may differ, as it will when applied to different vendors' systems.

2.1 VVPATs Are Not Forensic Audit Trails

The goal of Voter-Verified Paper Audit Trails (VVPATs) is an audit trail that can be counted to validate the machine's reported results, for example during a routine audit. These VVPATs do not provide enough information to be computer forensic audit trails [36, 37]. For example, they do not provide enough information to explain a discrepancy between electronic (computer-produced) and paper ballot vote counts. A forensic audit trail (FAT) requires data such as program traces [27] to answer such questions. Current e-voting systems do not record sufficient correct data for most forensic analyses (nor indeed, in most cases, do standards for producing that data exist [4]). Ideally, new e-voting systems will record this type of forensic data, but in such a way as not to violate laws and privacy concerns [30]. Balancing technical requirements and laws requires a systematic approach [28] that current e-voting systems appear to lack.

2.2 What Questions Can a Forensic Examination Answer?

In theory, an objective forensic examination of an election can:

- determine causes of unexpected and unexplained technical issues;
- settle questions triggered by a technical equipment performance problem, leading to broad acceptance of the ultimate report of election results;
- reduce or eliminate the need for a complete hand-count of affected ballots;
- stop wild speculations and the "rumor mill";
- reduce election litigation; and
- enhance the public's confidence in the election officials entrusted to conduct the elections and reduce reputation injuries fueled by lack of objective information.

Many of the most interesting questions are non-technical, and therefore a forensic examination cannot answer them. Was the election called correctly? This is both a legal and tecnical question. Can we correctly announce the winners now? This is both a legal and political question. Should we get rid of these machines or buy more? This is a question of business judgment. Should we sue someone? This requires legal, political, and business judgments. Integrating legal constraints into our forensic model is in the early stages of research [29], so we focus only on technical issues.

The forensic examination may answer many technical questions, such as:

- How many votes did the problem affect (minimum, maximum, best estimate)?
- How accurate are the (preliminary) canvass totals?
- If the totals are wrong, can the investigation recover the data (votes) needed to correct the totals?
- Is the computerized voting equipment operating in accordance with its documentation?

- Were any procedural guidelines violated that might have contributed to the cause of the problem?
- Does the problem affect only this jurisdiction, or might other jurisdictions have the same problem?
- Is there anything that appears to be evidence of negligence, malfeasance, misuse, or attack?
- What can or should be done to prevent the problem from recurring, in the short term (in the way of procedural workarounds) and in the long term (in the way of software or hardware changes)?

Election officials can use information and results from the forensic examination to help answer non-technical questions. They, or others, may ask the team to obtain more detailed information, including whether the examination discovered anything that might indicate a significant malfunction of the computer hardware or software, a deliberate attempt or successful) to affect the vote statistics or to interfere with voting, or serious errors in instruction manuals or documentation.

We begin by identifying the technical safety properties and security policies ("goals") that can appear within the fault graph.

3 When Should Election Officials Consider a Forensic Examination?

The requirements of an election with which this paper deals are:

1. *Accuracy.* The results of the election must reflect the votes cast, tempered by the requirements of the relevant laws.
2. *Availability.* The mechanisms for voting must be available to the electorate, so that all eligible voters may vote, and only those eligible voters may vote.
3. *Secrecy.* No voter may prove to a third party how he or she voted.
4. *Anonymity.* A third party cannot associate any particular ballot with an individual.

A forensic audit, by definition, is invoked when there appears to be some miscarriage of one or more of these properties. Any indication that one or more of these properties *may* not hold should trigger a forensic audit. Therefore, specific indicators that a forensic audit is necessary flow from the negation of one or more of the above requirements. Examples of such indicators follow.

The following problems raise questions about availability:

- Repeated "crashes," "freezes," or auto-reboots of any voting system component
- Components that become slower and slower the longer they are in service
- Unusual episodes of unresponsiveness that last more than a few seconds
- Failure of some usually reliable functionality
- Unusual or undocumented error messages from the application software of any component
- Unexplained and undocumented new system behavior, even if it occurs only once
- Failure of a post-election logic and accuracy (L&A) test of any component (especially if the same component passed its pre-election L&A test).

The following problems raise questions about accuracy:

- Any unresolvable failure of vote totals, ballot counts, or voter counts to properly sum and reconcile with each other, or with audit trail records
- Unusually high numbers of overvotes, top of ticket undervotes, write-in votes, or votes for minor candidates or parties
- Vote totals that are obviously too small (or negative), or obviously too large, even if they appear to reconcile properly
- Any inexplicable or illogical data (or indicators of data corruption), including in vote totals, database time stamps, or automatic audit logs.

The following problems involve both availability and accuracy:

- Memory cards or cartridges that, when read repeatedly, appear to give different results, or read errors
- Memory cards or cartridges that are supposed to be redundant copies of one another, but do not in fact contain identical data
- For direct recording electronic (DRE) systems, any discrepancy at all between the results reported electronically for a precinct and the results of a hand count of intact VVPAT records for that same precinct
- For DREs, multiple reinforcing reports of failure of the votes as recorded on the summary screen to agree with the voter's tentative votes or with the VVPAT
- For optical scanners, any batch of paper ballots that, when read repeatedly by the same or different scanners, yields counts that differ
- For optical scanners, any failure to scan and properly record the votes of a test deck that contains clean, correct marks.
- Multiple corroborating reports from voters, poll workers, or county employees that the voting equipment is not functioning properly (regardless of whether they explain the problem correctly.

The indicators for violations of anonymity and secrecy arise in one of two ways. If one looks only at the election, ignoring external data such as reports of vote buying and selling, then violations of these requirements involve

external markings that enable a ballot to be identified as unique. In the extreme, a voter may sign his or her ballot (in practice, this will not work in California, as any ballot with a signature is not counted), but more likely, a voter will vote in a particular pattern in some set of races to identify the ballot uniquely. So, one indicator of violations of anonymity and secrecy is a pattern of votes in races that are not duplicated among voters. An easy way to do this is to write in creative candidate names. Thus, one specific indicator is a large number of write-in votes, with each write-in candidate's name being unique.

Dozens of technical problems, major and minor, can occur during an election. The specific problems will depend on the particular voting technology used in the jurisdiction, the vendor, the software version and configuration, and the kind of election involved (general, primary, special, recall, plurality, instant runoff/rank choice, etc.). The vast majority of technical problems are simple, recognizable, and fairly routine, and can be resolved by standard procedures such as rebooting, replacing or recalibrating a piece of hardware, applying documented workarounds for known problems, or by conducting cross-checks, pre-election tests, and post-election auditing processes. Such routine problems are familiar to election officials everywhere and clearly should not trigger any formal examination in conjunction with an election. However, even in these cases, officials should save audit logs of appropriate subject and granularity to help analysts should a forensic audit be triggered, and to help determine whether the machines can be deemed trustworthy for future elections.

Further, sometimes an event occurs during an election that is outside the normal range of familiar problems. A system may crash, or yield inconsistent preliminary election results in one or more races. It may simply behave in an unexpected way not previously seen or documented (sometimes called an "anomaly"), and perhaps not repeatable. In fact, the very non-repeatability of a problem may itself be a key indicator that something more fundamental is wrong. Such unusual or unexpected events could result from a hardware failure, a ballot definition error, an operator or poll worker error, a previously unknown software limitation or bug, or a combination of such causes. Also, the possibility of election tampering through either malicious software or direct human alteration of vote totals cannot be casually dismissed. For example, a voting system problem is often dismissively described as a "glitch," "hiccup," or "computer error." In fact, unusual or unexpected events on a voting machine may indicate a problem, and should be examined.

Whenever a technical issue surfaces with voting equipment, election officials should undertake an inquiry as to its causes and cures. Even a seemingly small and inconsequential problem may actually be non-trivial and deserves examination; after all, in high assurance equipment, *any* error is cause for concern. Like the proverbial tip of the iceberg, small problems may be the only observable signs of large or systemic underlying problems. Even if the outcome of a particular race does not appear to depend on resolving the problem, conscientious election officials should examine it. This inquiry helps both the jurisdiction where the irregularity surfaced as well as other jurisdictions, for often, like icebergs, the underlying problem is present elsewhere but without visible symptoms or indicators—which might mean the problem goes undetected when it most matters. All unusual or unexpected events in voting systems, as in any high reliability, high security computerized systems, should be examined. A forensic examination of the computerized voting system components related to or potentially affected by the problem may prove helpful, or necessary, under these circumstances.

4 Laocoön: A Model of Forensic Logging

We have developed a model of forensic logging, called Laocoön. Laocoön takes as input a set of security policies and general information about a system's architecture, and gives a set of directives for data to log as outputs, including means of logging that data in which unrelated can be pruned. The result of using the model is that it can aid in understanding and linking events into steps of a system failure, and helps to place bounds on the conditions that lead to an unusual or unexpected step in a failure. The fault graphs used by Laocoön can be partially derived by reverse-engineering configured policies ([31], §8.2), and the conditions describing the graph are translated into logging requirements. When implemented, the system can record forensic data at various levels of granularity, in standardized and parsable formats.

Applying Laocoön to a system does not preclude the use of a skilled human analyst. Indeed, an analyst is still necessary to interpret the data. However, by involving the human analyst in determining what data should be collected, the data is more likely to be present, and of value, when needed. Further, by using a systematic approach to instrumenting a system to collect logs, rather than analyzing an ad hoc collection of unrelated logs, not intended to be used for forensics, the chances of collecting the necessary data are increased.

The results of experiments that we have previously applied Laocoön to have shown promise [31, 26], and thus in this paper, we expand our approach to look at voting systems. Indeed, voting is in many ways an ideal approach to this method because in theory, the modes of operation of the machines are limited, and the security policies well defined. Indeed, only systems that exhibit limited operation and well defined policy are appropriate choices for voting machines.

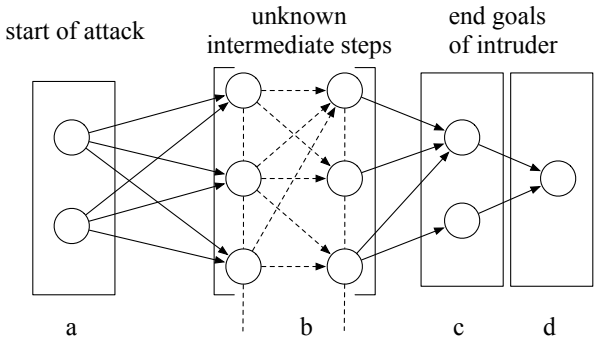

Figure 1: Diagram of a generic failure or attack where circles represent actions. A failure model almost always consists of at least the endpoint (d), but may also include the beginnings (a) and possibly other states near the end (c).

The design of an ideal audit system for computer forensics (including, but not limited to e-voting) begins with requirements. The requirements are translated into policies and the policies are used to define failure graphs. The failure graphs are formed by starting with the predefined policy violations (e.g., a recorded vote changing) and working backward to the point of "entry" into the system or the starting trigger of a series of events, as illustrated in Figure 1. Each node ("goal") is described by the preconditions required to accomplish an event to achieve the goal, and the post-conditions of achieving the goal. As mentioned earlier, we cannot define, let alone enumerate, all *methods* of violation. The model tolerates this by using data about steps toward the policy violation that we do know something about to place bounds on the steps that we do not know anything about (Figure 1b). These fault graphs are then translated into specifications and implementations that Laocoön uses to guide logging—what data to log and where to place the instrumentation to log the data. Finally, that data is used by a human analyst to conduct forensic analysis in a rigorous and systematic way.

For example, consider how Laocoön would guide the logging for an analysis of over-voting. Over-voting occurs when a voter selects more candidates than allowed in a given race. Electronic voting machines generally prevent voters from over-voting, which means that ballots recorded with over-votes indicates that the software designed to prevent over-votes failed, leading to a forensic audit. Such an event could ultimately be recorded in a limited number of ways, either on a VVPAT or on electronic media. At some point, the value of a variable or a (set of) bit(s) changes somewhere. This requires the manipulation of a limited number of data points. We need not describe in advance *how* the data is manipulated (and in fact this may be impossible). It is sufficient to understand the possible paths that lead to this manipulation. The paths begin at entry into the system (e.g., touchscreen, supervisor machine, hardware manipulation) and end at the data. In between represent events such as specific library calls or system calls. The paths in between the endpoints must be monitored (e.g., via kernel modifications or virtual machine introspection). This automatically places bounds on the intermediate steps in the path. This allows a system to collect enough information for a forensic analyst to analyze the violation—the traversal of that fault graph—and either understand what happened, or determine how to analyze the system further to obtain any necessary information.

Unfortunately, most of the time, systems do not record sufficient data to validate the correct operation of an electronic voting machine, or to determine the cause of incorrect operation, when an anomaly is discovered. There are at least two consequences of this: first, machines that do log the necessary information can be created by applying the model during the design phase. Second, we can identify points in the election process at which additional (or better) data may provide information enabling the analysts to determine which among multiple causes and effects are the causes and effects of the aberrations noted. This is an advantage of applying the model because it can remind analysts (and therefore also election officials and ultimately the public) not to draw conclusions too quickly, since other possibilities may exist. For example, examiners of the Sarasota, Florida, election for Congressional District 13 in 2006 never proved what happened to the 18,000 missing votes. They were able to eliminate some possibilities, but the question still remains whether the problem was poor ballot design or something else.

5 Application of Laocoön

In this section, we describe how to apply Laocoön to obtain detailed information about what data the forensic audit will require. Critical to the analysis is that the data be *meaningful*, that is, it provides the information expected; and that the data be *assured*, that is, preserved accurately. We deal first with meaningful data. We then focus on its assurance.

5.1 What Data to Preserve

We now apply Laocoön as a framework for analysis, beginning with voting machine requirements. Much of the data to be preserved covers multiple requirements. For example, the memory cards used in the systems may provide information dealing both with availability (memory cards with dirty connectors causing intermittent failures) and accuracy (memory cards with bad memory causing

errors in recording votes). In what follows, we associate components with indicators.

Repeated crashes, freezes, or auto-reboots may indicate a failure within the system, and describe a goal state of the fault graph. Therefore, the model states that data to describe the system and the failure should be recorded. Thus:

Rule P1. Record the indications of any failure—what happened, when it happened (specifically at which step in the voting process), any error indicators such as a message on the screen, and so forth.

This includes system level events as well as human events, such as someone using the machine. For example, if a possible failure includes a shutdown, then record the programs or commands capable of issuing a shutdown. If a failure includes wiping the memory of the system, then record commands capable of performing such deletions, as well as the permissions used to issue the command.

Likewise, starting at the beginning of the fault graph (rather than the end goal states) suggests:

Rule P2. Record information about the entry points into the system, including the locations from which people accessed the system (for example, through the voter interface or by opening bays for maintenance).

That must include non-voters, such as election officials, delivery personnel, and voting system vendor employees. It also includes visual descriptions of the state of the entry points, including any available screen shots. For example, since lightening strikes, floods, or someone tripping over a power cord can clearly result in a system failure, record environmental data: location of power cords, weather (detailed records of temperature and humidity and other factors).

As part of Laocoön, one must analyze the set of possible paths from the initial states of the graph to the terminal (error) states. This requires more data:

Rule P3. Collect any external data relevant to the state of the voting system.

Obvious examples are VVPATs, audit logs, memory cards and other removable peripherals such as USB sticks and cables indicating connections to telephone lines or networks. Anything recording the externals of the system, such as videotapes from security cameras, will prove useful. Finally, people are an excellent resource here because they may have information and not realize it. So note (and possibly interview) poll workers who set up the machine, and the number of voters who interacted with it (e.g., from poll books). Chain of custody details for the voting machine and peripherals from when they were initialized will provide more information, as will records of tamper-evident seal numbers (and of course any breaking of those seals).

When components (such as VVPAT printers) become slower or exhibit episodes of non-responsiveness, the same elements that would be recorded for the primary system should be recorded for the component attached to the system. This includes any modification or replacement of a particular component attached to the primary machine. Also record the reason, if known (for example, the primary is non-functional, or the thermal VVPAT tape was adjusted, jammed, or had to be replaced).

When discrepancies occur in the totaling of votes, the fault graph developed using Laocoön shows the paths that lead to those end points. To select among these paths, data needed includes the records of how many ballots were cast, spoiled, and provided to the polling stations; "zero tapes" that suggest whether the e-voting systems had any votes on them before the polls opened; the end-of-day tally sheets and signed poll-worker records indicating how many voters came. Additional data comes by eliminating potential initial points. Among the data to do this is the chain of custody for all devices and storage media in the path that the ballot takes—this includes the system on which votes are cast and the memory recording the votes cast. This also includes details about the e-voting device itself so that officials can determine if the problem is confined to a precinct, a race, a single party in a primary election, one jurisdiction, or a particular machine or a particular type of machine. For example, if it occurred in only one race, then the problem is likely related to some attribute of either the race (perhaps many voters did not want to vote for some unexplained reason), the ballot layout (perhaps many voters missed seeing the race on the ballot), or the systems used (perhaps touching the location of the race on the screen triggered a bug in the firmware that caused the vote not to be recorded).

If concerns about secrecy and anonymity arise, Laocoön suggests looking for anything that identifies the ballot uniquely, and that associates it with the voter. Thus, any unique item or number or code being given to the voter will prove helpful and should be recorded (*not* what it is, though—otherwise the forensic audit itself compromises secrecy and anonymity). Similarly, patterns in ballots as discussed above make the ballot uniquely idenifiable, so ballots as a whole should be preserved. (In California, provisional ballots may not be cast electronically. Otherwise the names associated with them—for determining the legitimacy and/or legality of the vote—also reflect a method for compromising secrecy and anonymity.) The dissemination of such unique identification can be used to trace its use later in the fault graph by looking through logs for evidence of communication of the unique identification. In this context, examining the physical layout of the location of the voting system may prove fruitful, because some voting systems emit audio signals that an attacker can capture remotely [7].

Equally critical is:

Rule P4. Record any signs that the data is incomplete or may not be trustworthy.

For example, if the system is supposed to record every occurrence of a particular event but does so only intermittently, that indicates a problem that may interfere with the correct operation of the system, and almost certainly will interfere with the forensic analysis of that system. We now examine this point in more detail.

5.2 Assurance and How to Preserve the Data

Forensic analysts can draw credible conclusions only from trustworthy forensic data. This property is *assurance*—confidence that the data meets a set of requirements "based on specific evidence provided by the application of assurance techniques" ([6], §18, p. 478). In this case, the requirements are that the data accurately reflects the state of the system when it is recorded, and the data is not changed from the time of recording to the time it is used in the forensic analysis. It also reflects that the forensic log data can be mapped back to the system's design specification to determine where—and possibly how—the system may have deviated from its intended operation.

The first requirement speaks to the integrity of the system and what the data being saved represents. As previously argued [30], existing e-voting systems do not generate forensic information. Therefore, the forensic analysts must try to deduce information from the recorded inputs and outputs of the system, knowing how the system works.

In technical terms, Laocoön requires that the data be recorded at failure points, both temporally and as close as possible to the artifact that fails. This translates into the procedural rule:

Rule A1. Preserve all artifacts as soon as the problem is discovered, in the state in which the problem was discovered.

In practice, if the problem occurs during the election, officials must continue to use the equipment because they cannot stop the election. In that case, copies of the data on the equipment—for example, making clones and/or backups down to the contents of the disks and memory (because some tests and analyses will destroy data in memory or on disk)—will preserve much of the information for the examiners. Where circumstances prevent freezing or capturing the evidence (such as an error message), a digital photograph will help document events and contexts for later use.

Preserve all voting system equipment, including the precinct devices (e-voting machines, printers, monitors, registration check-in devices, etc.) as well as county-level devices (card readers, ballot counting devices, servers) until the examiners and officials determine the scope of the review. Further, if a computer or device involved in the election is running at the time the problem was discovered, it is best for the examination if it is left running so that, for example, examiners can determine what software was running when the problem was discovered. If the device or computer was off when the problem appeared, it should be left off.

If the machines are connected to a network, forensic experts will decide what to connect to, or disconnect from, the network. The network containing machines involved in the election should not be altered [25]. If this is not possible because, for example, the machines are at a polling station, officials should keep detailed records of what staff did and any events that occurred after the problem was discovered. The physical environment in which the equipment was located should be left undisturbed or, if that is not possible, photographs and measurements should be taken.

Maintaining the provenance of these artifacts becomes critical. Especially in a situation as volatile as an election, observers may want (or need) to validate the examiners' conclusions. If the preservation of the evidence is questionable, then the results of any forensic examination relying on their data also becomes questionable, by Biba's model [5] and Rivest and Wack's notion of "software independence" [33]. Thus, minimizing the handling of these artifacts, and tracking their chain of custody, provides a basis for assessing the trustworthiness of the transmission of the artifacts.

Rule A2. Election officials must have a process documenting how to handle potential evidence.

If people do not believe the evidence has been preserved, they will question the validity of the examination's conclusions. Here, the "chain of custody" records figure prominently. In a forensic examination, by applying Laocoön to humans, one can map the chain of custody records both to other observations from humans ("when I first saw the machine, it had blue tamperproof tape, and now it's red") as well as to forensic logs. In addition, no one should ever be left alone with potential evidence including chain of custody records. This "two-person rule" means that at least two people can vouch for the accuracy of the chain of custody records. This rule applies to original evidence; of course, one person can handle copies of evidence alone. Ideally, some technical measures would make evidence tamper-evident (e.g., cryptographic hashes on log data [34]) or fault tolerant (e.g., streaming to a separate system [40], perhaps in a separate security domain). However, systems currently do not have such measures, so

the human procedural steps are necessary. In most cases, the integrity of the data will be the only constraint, but depending on the type of data, privacy may require confidentiality. In those cases, officials and examiners must disclose the reasons for keeping some of the evidence confidential, and the basis for selecting the evidence to be kept confidential.

Rule A3. Potential evidence should be frozen and secured.

Once it is clear a forensic inquiry will be convened, only forensic examiners should touch any of the equipment or files. Everything connected with the election should be frozen and maintained as close as possible to the state it was in when the problem was discovered. Preserving the environment and materials extends to the computer environment. No personnel should create, open, edit, or delete files, run programs, log in or log out. Further, this all must be *observable* so the public can see the rules are being followed.

The next two rules are related:

Rule A4. The process for preserving evidence must be public.

and

Rule A5. The methodology and results of the forensic examination must be public.

The level of assurance is determined by evidence that convinces those who require the assurance. As elections are held so that the public at large may determine the winners, the public is the body that must assess the assurance of the process of forensic examination. If an examination is conducted in secret, often the public response is to doubt its results, regardless of how well the evidence was preserved. Elections in the United States are traditionally conducted openly, with a minimum of secrecy (for example, in some states, observers can view every step of the process except the voter casting her votes in the booth). This expectation of openness naturally extends to examinations of equipment issues that could affect election results. Thus, the public should be able to observe all activities before and during the examination. Of course, this openness needs to be balanced with the need to maintain the confidentiality of examiners' discussions as they are conducting the review, and to protect the vendors' proprietary information. For example, the California Top-to-Bottom Review [7, 11] used cameras to broadcast video to a public area apart from the secured facility where the "red team" analysis was conducted. However, no audio was broadcast. Any member of the public could thus come to watch the examination—and the examiners could speak freely about confidential information and their testing and preliminary conclusions, without premature disclosures.

In addition, the composition of the team and the conditions under which they work are important. The following flows directly from the above five rules.

5.2.1 Providing a Facility

Depending on the scope of the forensic examination, the team may need to work at a physical facility with controlled access, such as a conference room or some office space that can be locked and has alarms. The members of the forensic team must control who is allowed to access that space. It will need to be large enough to house:

- Paper and other physical evidence
- The computers involved in the examination; the team can determine whether all computers need to be housed in the space concurrently
- Any other equipment relevant to the examination or that the team needs (for example, cameras, recorders, printers, laptops, etc.)
- The people on the team, as well as any other authorized personnel such as observers.

The team will need an office safe to lock sensitive material such as notes, disks, and laptops when their protocol requires it, or when no one is present. Past examinations have found something on the order of eight cubic feet of locked space to be adequate.

Within the secured space, the team will need access to the Internet for sending and receiving email and for making Web searches (which can be helpful when conducting forensic analysis). Under no circumstances will they connect any voting system component to the Internet. No voting system component should ever be connected to the Internet, even during forensic examination. Depending on the type of problem, the forensic team may need to connect the voting system components to one another or to their own computers for diagnostics, which will require one or more internal networks within the secured space. The best way to guarantee network security in the secured space is by keeping all other networks physically separated from the one connected to the Internet.

5.2.2 Team Organization and Size

Depending on how many different types of devices or how much software is involved, some inquiries may need more people, more time, or consultation with other experts. Many technical issues, perhaps most, are caused at least in part by the failure to follow some procedural requirement for setting up and using the computer-based equipment. Thus, except when unusually complex events occur, a team of two to four people will usually suffice but they all must bring special expertise to the project. Occasionally only one well-versed individual has been

contractually brought in for a forensics review—for example, a computer science professor with experience in voting systems who was supported by graduate students. Normally, team members will be a group of individuals recruited by a project leader appointed to head the inquiry [7, 38, 35, 13, 15], or from a single firm [32] contracted for the purpose of the inquiry.

5.2.3 Technical Qualifications

A good team brings a special set of talents and skills unusual even among experienced programmers. Team members will need to learn their way around a complex system that not only did they not help build, but may have never previously seen, and in a very limited time. They will have to quickly discern the design principles and conventions used in building the software and hardware, and its likely strengths and weaknesses. There is always the possibility that a deliberate attack by either outsiders or insiders [8, 9] caused the anomaly. Only an expert will have the knowledge and tools to determine what happened in those cases. Business, educational and other governmental entities' computers have become frequent targets for attacks, and this possibility also exists for elections.

All types and components of electronic voting systems, including optical scanners, DREs, automated ballot marking devices, and their election management software, are complex computer systems. They use a wide variety of technologies such as memory, operating systems, applications software, programming tools, databases, and security and cryptography. Obtaining a correct architectural and operational understanding of how they work together is the grounding for the forensic examination. The nature of these software programs greatly complicates a team's quick grasp because these large programs are usually written in pieces, at different times, by different people, in different programming languages, and use specialized technologies.

Despite the apparent simplicity of the concept of voting, a computer-based voting system is actually extremely complex technically, far beyond what most people, even highly experienced elections officials, are likely to appreciate. A DRE may contain as much as 300,000 lines of software code. The canvass server, with its operating system, database system, and election management system, has considerably more lines of code controlling its activities. All of this code is woven together from modules written at different times by different people in different programming languages.

To obtain this system comprehension, the team must have the capacity to read and analyze the systems' source code, and from that determine the functionality of the system. At least one—preferably two—team members must be experts in computer security and forensic analysis. Understanding most common error messages and familiarity with most common forensic tools simply is not enough [29]. It is not necessary, or sufficient, for the team members to be "certified" by various companies or institutes such as CISSP, GIAC, or SANS. But the team must know, or be able to learn quickly, how to set up the systems in question, and how they could be set up in other ways (this will help them uncover problems arising from not following recommended set-up procedures); how to recover deleted files; and how to make copies of the systems' memories and disks without disturbing the contents of the original memory and disks in any way. As an example, for Windows-based election management systems and canvass servers, the team will need to access the multiplicity of logs that Windows keeps. As another example, the team may have to set up tests to analyze the voting system software and observe its execution in order to test possible causes of the problem. This would be done on copies of the systems, not on the actual systems. A good forensic team can perform these tasks.

To conduct these analyses, at least one team member should know the architecture of one or more voting systems. Individuals who have participated in reviews of these systems, or who have studied reports describing the architecture, source code, operations, and vulnerabilities of deployed voting systems, or who have co-authored these reports, will provide significant insights into the use and examination of these systems. They will be able to use their experience and knowledge to diagnose problems and identify solutions more quickly than examiners without this experience and knowledge. But other computer scientists, software engineers, or computer security and forensics firms could get up to speed by studying the published voting systems studies (see Appendix 2).

Finally, at least one team member must have expertise in election administration and procedures. Election management is a legally intensive and unusually complex set of time-bound interconnecting processes that must sequence almost perfectly for the election to be conducted successfully. As officials know, ballots and voting machines must be properly configured, tested, and delivered on time, with poll workers properly trained, voting locations open on time, tabulation equipment functioning properly, and all memory media and voting data returned promptly—and each of these tasks requires a myriad of subtasks to complete in sequence. Normally, an election forensic examination is also conducted under severe time pressures, and there will be little time to explain and bring team members up to speed in the nuances involved in election administration. With a team member well versed on these essential administrative points, the review can be conducted far more quickly.

5.2.4 Non-Technical Qualifications

As with examiners or auditors in any other field, at least three qualities are essential: objectivity, the freedom and willingness to follow the inquiry wherever it goes, and the ability to describe the causes of the problem completely and accurately without regard to potential organizational embarrassment. In sum, the forensic team must have independence.

Strong ethics are essential: the forensic team members must have neither conflicts of interest nor the appearance of conflicts of interest. If at all possible, they should be entirely disinterested in the results of the election being examined. If that is not possible, the forensic examiners must be able to set aside their interests and undertake the examination without bias. Otherwise, the results will not receive the trust and legitimacy needed by all parties, including the public.

The need for independence and avoidance of conflicts of interest leads to the necessity of excluding from the forensic team governmental IT employees (county or State) and representatives from the voting system vendor. The county or election office IT personnel who helped run the election, and the vendor technical representatives who know the systems intimately, are crucial resources for the forensic team, but their role must be limited to providing information to the independent forensic team. This role is discussed in more detail below.

Finally, the team members must be persons of high integrity and good judgment, and must not be associated with any partisan organization involved in the election. There may be a great deal at stake in the resolution of an election problem. The outcome of important races may hinge on the results of the inquiry. The problem may have besmirched the reputations of election officials, the vendor, and other participants. The problem may have shaken the public's confidence in the election. The members of the team must have the temperament to be rational, fair, and restrained in their demeanor when writing and speaking about the examination. They need to be able to put aside any opinions in order to find the truth in the inquiry, wherever it lies.

5.2.5 The Role of the Vendor

Cooperation of the election systems vendor is critical to the examination's success and credibility. The vendor can promote a positive public perception of its company despite the technical problem if it fulfills its unique role as a resource and support for the team. However, a vendor should be considered no more special than any other poll worker or election official. For example, under no circumstances should an election jurisdiction forego a forensic analysis of a problematic election because the voting equipment vendor opposed it or suggested an explanation for the problem. Nor should the vendor apply pressure on a jurisdiction to accept its explanation and bypass having its hypothesis independently confirmed. The "two-person rule" rule mentioned above must be applied to the vendor, like everyone else.

Though the vendor is critical to the success of the forensic review, the public agency must not allow the equipment vendor to appoint any examination team members. The basic rule is: the vendor must be a resource for the team, but must not conduct or participate in conducting the examination [3, 21]. Four important reasons lead to this conclusion:

First, the vendor is a privileged insider. Its in-depth knowledge of the systems will be valuable. But that can also represent a threat based on their knowledge of the system and access to it. Thus, as both our model of faults and attacks, and our models of insiders and "insiderness" [8, 9] suggest, the vendor should understand the possible entry points to a voting system at least as well as anyone else. Any procedure (e.g., hardware installation/removal or software command) suggested by the vendor should be carefully considered by the forensics team *and* carefully documented.

Second, forensics team members must approach the examination with no preliminary conclusions of what caused the problem. In practice, this means they must be prepared to follow the evidence. An examiner who has a "pretty good idea" of what happened, and why, before the investigation begins may be predisposed to overlook and misinterpret data. The vendor representatives are likely to focus on causes unrelated to problems in the vendor's products or recommended procedures. But a vendor can and should communicate its hypotheses to the team, so the team can determine how and to what degree they should explore these ideas.

Third, voting equipment vendors have a direct conflict of interest. Certain types of diagnoses and conclusions will not assist the financial interests of the vendor. Thus, the human and business tendency is to try to identify some explanation other than, or in addition to, equipment problems. In some cases, the equipment will be blameless, but in others some aspect of the vendor's activities—perhaps in programming, or in supplying correct documentation—it will have played a major role in the technical disruption. The examination should not be biased either way. If a vendor conducts the examination, a significant portion of the voting public will not respect the examination's conclusion despite ample supporting evidence simply because of the financial conflict of interest. The presence of this conflict taints the integrity of both the examination and the people who selected the examiners. It is better to avoid the problem by having an arm's-length examination.

Fourth, the vendor plays a critical role as an information resource. The examiners will need to learn exactly

how the specific equipment is set up, how it is operated, and how the software works. Often, a day spent talking with the vendor personnel can give the team insights that will speed the investigation greatly. We emphasize that the purpose of this vendor communication is to guide the examiners' understanding of the system and its use, and only that. The vendor should endeavor to fulfill this vital role that it uniquely holds.

The team's communication with the vendor must be handled carefully, to preserve the public perception of the integrity of the examination, as well as its actual integrity. The team must be free to communicate with the vendor for technical information, but if at all possible the convener-sponsor of the examination should also be present. If the vendor wishes to communicate with the team, it should do so through the sponsor and not contact the team directly. This arm's-length relationship may seem extreme, but it prevents the vendor from applying any pressure on the examiners and further promotes the review's integrity.

The vendor must be allowed to respond to the forensic examination team's report. The vendor response must be separate from the examiners' report, to emphasize the independence of the investigation. Whether the vendor's response is to be made after the examiners' report is publicly issued (as was done in the California Top-to-Bottom Review [7]), or whether it is to be given to the examiners before their draft is made public so the team can take the vendor's comments into account (as was done with the RABA review [32]), is something to be decided and recorded contractually. The advantage of the former is that the public will understand the vendor played little to no role in the investigation; the advantage to the latter is that possible factual errors (such as erroneous information from second hand information) can be identified and more fully researched so the final report is completely accurate. As long as the team's independence and integrity is not simply assured, but also perceived as assured, either method works.

The vendor is a critical and key resource for the examination, and must be engaged to provide the examiners with technical and procedural information about the equipment and how to use it. If the vendor promptly and completely supports the examination, the vendor will be, and will be seen to be, an asset to the examination. It can credibly present itself as a company concerned about the quality of its products, their correct use, and the larger public trust embedded in the elections process.

6 Legal, Contractual and Practical Issues

6.1 Overview

Voters place great importance on the integrity of their election processes. So election officials provide the best assurance to the public when they take an immediate, vigorous public stance detailing the steps to examine the technical irregularity and its impact ([21], Appendix A-1, p. 371). Yet before forensic examiners can begin work, contractual and legal issues must be resolved. If the outcome of an election hangs in the balance, delaying the evaluation by even one week can be too long.

The best plan is to prepare in advance a sample set of fair and responsible contractual terms for a forensic inquiry [7]. The contractual issues are generally similar whether the forensic team is from a private firm or is a team of independent scientific experts, regardless of who retained the examiners (e.g., county election officials, a Secretary of State, a court, or some other authority). The following discussion simply provides an overview of some contractual and legal issues that will arise. It is not intended to provide legal advice or an exhaustive review of all the law that may govern or the legal issues that could arise; for such, legal counsel should be sought. Its length derives from a desire to help others avoid the weeks of difficult contractual negotiations that have delayed some previous examinations.

6.2 Preparation and Stakeholders

In a small local election, county election officials may be the sole decision-makers of whether to convene a forensic inquiry. In federal elections, such as the presidential election, the decision over what type of inquiry and what credentials team members need will often involve national political parties, presidential candidates, the Secretary of State (or other chief State election officer) along with the State Attorney General and county attorneys, all negotiating a process for forensic review. This wide involvement owes in part to the legal fact that our elections are conducted under an interwoven fabric of Federal and State law and are intensely political processes.

The importance of elections and their relation to control over the levers of power can lead to the remote possibility that prosecutors of either (or both) Federal or State/county government will intercede where unusual technical events occur, perhaps to attempt to block an examination convened by the local officials. The increasing frequency of documented unexpected technical events, however, actually tends to reduce the likelihood of prosecutors becoming centrally involved, an ironic silver lining for public transparency. When prosecutors move in and assume investigatory control, closing out public access and transparency, the rumor mill and conspiracy theories often take over. Public confidence in the integrity of the election and its administrators can plummet even if later the officials are exonerated.

Fortunately, most prosecutors have sufficient experience with computers and computer forensics to know that

computers are far from infallible and that technical irregularities during elections are far more likely to occur for reasons such as programming errors rather than deliberate cyber attack or criminal conduct somewhere within the election administrative system. Knowing the public's inferences—of presuming criminal conduct when formal prosecutorial investigations commence—prosecutors may rather choose to seek involvement in helping to structure a qualified independent forensic examination whose report will also come to their office as well as to the election officials and public. Further, they may seek an informal or formal agreement concerning the handling of evidence (ensuring that if evidence suggesting deliberate wrongdoing is discovered, it will be preserved in a legally sound manner), and the duties of examiners to report potential wrongdoing.

Regardless which stakeholders seek to play a role in determining the scope and composition of a forensic inquiry, election officials will want to ensure that they are fulfilling all obligations imposed on them by law, including any fiduciary duties for assuring an accurate election.

6.3 Timeline, Authority, Scope, and Public Relations

Timeline: In most election forensics examinations, the resource in shortest supply will be time—especially if the outcome of a race is in question. Forensic examinations frequently take several weeks; particularly difficult ones may take two months. It is essential to plan to devote the time (and funds) needed for a quality review. A good forensic team may decline the job if the schedule is too compressed for the job to be done properly. If the outcome of a race is in question, a target date should be set in the contract for completing the examination, with some flexibility for adjustments. If no race results are drawn into question, it may be possible to have a more open-ended examination in which the timeline remains flexible according to what is found.

Authority: Election officials possess legal authority over the election equipment and materials. But a court, prosecutor, or legislative inquiry might displace their role [1]. It is understandable that government officials will want to be involved and remain informed throughout the process since they have the ultimate responsibility for the proper conduct of the election. But the forensic team needs freedom to act within its charge according to its own direction and schedule. It also needs to be able to ask questions of anyone who might be able to provide information, including election officials, vendor employees, poll workers, and even voters. These access points for relevant evidence need to be stated contractually.

Scope: All parties will need to agree on the goals and parameters of the examination—what they can and cannot do. That way, all parties are likely to understand their respective tasks and responsibilities. Experience has shown that examinations have difficulties when these parameters and goals are not agreed to before the team begins its work. But the scope of a legitimate forensic examination has to be very wide and open-ended. If a forensic examination is called for at all, the problem by definition defied easy explanations and diagnoses. The examiners must not be limited, for example, to examining the hardware or software of just one component of the system, nor can any component be excluded from examination; once the review is underway, however, and initial diagnostics are complete, reviewers can often narrow the scope and not need to review all components.

Within reason, the team needs the authority to go wherever the examination leads. In the course of their examination, the examiners may come across potential problems in the voting system that in the end are not related to the problem that prompted the examination but which had to be pursued until they could be eliminated as a contributing cause. While the forensic team should generally stay within the scope originally assigned, the contract should specify that they must report significant flaws or vulnerabilities they happen to discover in the course of their work whether within the scope definition or not. The scope's limitations can also be stated, such as if evidence of malicious code or other attacks is found, the team is to notify the legal counsel or the prosecutor's office that the jurisdiction has designated.

Public relations: The public has a legitimate strong interest in election accuracy and thus in obtaining knowledge of the outcome of forensic examinations. In the election context, for efficient and accurate communications, the contract will specify a single point for communication on both the examination team and the convening government entity to which the team will report. An update frequency might be specified, including whether the team spokesperson will be expected to communicate directly with the public via media events after the report has been submitted. This agreement should balance the need of the examiners for freedom from interference, and the needs of the candidates, the vendor, and the public to follow the examination's progress and learn its results.

6.4 Indemnity, Nondisclosure, Statutory Barriers, and More

Indemnification and Costs of Defense: A settled part of agency law requires indemnification of agents for reasonable costs incurred that are attributable to the agreed work [2]. Like other agents, the forensic examiners will

expect to be shielded from any lawsuits that might result from their work, provided their reports are not slanderous and they obey the other contractual clauses. Quite often, this protection can be provided easily by explicitly stating that the forensic examiners are acting as agents of the county or State government [38] that conducted the election and that costs of defense will be assumed by the government entity. Under some State procedures, the forensic examiners may be protected as agents of a court that orders the forensic examination. The lawyers for the election jurisdiction that retains the team will need to research and provide fair indemnification and cost of defense terms, for without it the effort to recruit qualified professionals can be severely impeded.

Nondisclosure Agreements (NDAs): Often, a voting system vendor and the government agencies that procured the equipment have agreed to be covered by a nondisclosure agreement. Leaving aside the question of whether there should be NDAs for publicly deployed voting system technology, such terms are a part of some procurement contracts. It may be necessary that these NDAs be extended to cover the forensic examiners. The forensic team or their firm will usually be willing to sign a narrowly drawn, limited NDA to protect the intellectual property of the vendor that is not within the public domain. (Appendix 1 provides an example.) But most experienced forensic teams will refuse to sign any broadly worded, unbounded NDA since it may expose them to unnecessary liability and could impede the forensic examination report and conclusions from becoming public. If, as has occasionally occurred, a vendor objects to anyone other than the government employees of the election jurisdiction conducting the examination and claims that an existing NDA bars such access for retained experts, the contractual classification of the team members as the jurisdiction's "agents" is often enough to eliminate any difference in access between the team and employees. In the next generation of voting equipment procurements, purchasers would be wise to include provisions specifically authorizing forensic examinations and the NDA terms, if any, when officials choose to convene an inquiry.

Confidentiality and publication: The public has a strong interest in the publication of a detailed report on the team's findings. The only information that normally should be withheld in the published forensic examination report is information that either: (a) is legitimately proprietary to the vendor and not in the public domain or available beyond the vendor's personnel, or (b) concerns specific details of security vulnerabilities that might be exploitable in an election in the near future, before the problem can be corrected. The exploitable details of security vulnerabilities should be written up in a separate report that is not made public, but the recipients and protections for this confidential report should be described in the contract. The scope of "proprietary information" should be defined so that it cannot be interpreted to bar from public access the forensic examination's general findings. One approach would be to incorporate by reference the "industry standard" of disclosure that the California, Florida, and Ohio Secretaries of State and vendors agreed to in the reports under those offices' sponsorship (see Appendix 1). An additional clause to promote the larger public interest in the availability of important information would specify the public agencies to which the report will be submitted, including, for instance, the U.S. Election Assistance Commission (EAC), National Institute of Standards and Technology (NIST), National Association of State Election Directors (NASED), and the State's chief election officer.

Examination security: A forensic examination must be conducted under secure conditions [20]. The specific expectations should be listed in the written contract. Frequently, the security precautions required for access to voting systems and ballots (such as the two-persons present at all times rule) should apply to the forensic team as well. Depending on the nature of the examination, the necessary security may require special secure environments to be created in which to do the work, with key control, video surveillance, guards, and so forth. The costs for these arrangements must be borne by whatever agency is in charge of the examination. Team members must also protect the intellectual property of the vendor, particularly any vendor-owned source code, both during and after the examination. Finally, the examiners must take steps to prevent any exploitable security vulnerabilities they may discover from becoming public knowledge.

Technical resources: The forensic team will request tools and resources as needed, and will need to receive them in a timely manner. These requested resources are almost certain to include the source code because that is the set of commands for the computers under examination. Normally, all parties (officials, courts, vendors, and others) should seek to expedite the review and supply the resources under their control. Any problems in providing those resources will impact the delivery date of the forensic report, and possibly damage its credibility. Contractually providing all parties with a mandatory timetable and prompt follow up procedures when delays occur may help keep the examination on track.

Role of vendors: The vendor's important role was discussed above, but a few points will be reiterated here. The forensic contract or an addendum contract between the public agency and the vendor should specify the roles the vendor will play, including the timetable for vendor supply of specified resources, technical support, and permission for team access to the source code and build

environment. It should record the decision regarding the sequencing of the vendor's receipt of and opportunity to respond to the forensic team report. The primary choices are for the vendor to receive a draft with an opportunity to respond to the forensics team pre-release, or to receive a copy post-public release. Another clause should detail how the vendor's response will be treated (e.g., a posted link accompanying the team's web-posted report). The contract should clarify the types of contact the team may have with the vendor, and specify the terms for the arm's-length relationship with the vendor, including the vendor having no role in the forensic team's assessments other than suggesting potential causes for the problem.

Vendor cooperation can greatly enhance the speed of the forensic review and lower its costs [18, 17]. Such cooperation can ultimately promote the vendor's opportunities to benefit from the examination. Vendors who quickly authorize source code review (under carefully constructed legal terms) and deliver the necessary materials can profit from learning whether there is a problematic point so that it can promptly be corrected for other jurisdictions/customers within the governing certification regime. Public authorities can (and, we believe, should) praise the vendor for speedy and complete cooperation in the forensics review.

To further promote this arm's-length relationship and avoidance of conflicts of interest, the vendor should not directly pay for the examination although, in some cases, depending on the State and forensic conclusions, it may be appropriate for government authorities to charge back to the vendor part or all of the expenses.

Costs: The cost of an examination can vary widely, and a budget must be agreed to as a part of the contract. The cost will vary depending on who conducts the examination. A forensic or security firm may charge more than academics who use the opportunity to involve graduate students, but a private firm may be able to sign a contract quickly. Costs, of course, rise with the complexity of the examination, the security arrangements required, and the travel necessitated. HAVA funds have been used for voting equipment reviews so this may be one source of financial support.

7 Conclusions and Future Work

Forensic analysis is generally difficult [24]. In particular, forensic analysis of e-voting machines poses many challenges. In comparison to traditional computer forensics, it has more tradeoffs and even outright contradictions. It is of course much more nuanced than auditing paper ballots, although the high-level techniques are surprisingly similar. Recent history counsels that some jurisdictions will continue to experience serious electoral complications going forward. The job of the elections official has never, we think, been more important.

It is no longer sufficient to rely on current technology and practices. We must use not merely good design and forensic practices but rather the rigor of high assurance in design and analysis that would go into designing mission-critical systems such as those on military aircraft or satellites.

One of our future projects is to compare the requirements to how elections are run, and to focus on the design and implementation requirements of both the process and the machines to enable us to answer the questions that we have posed. We are also looking at applying high assurance techniques to e-voting, which will require an analysis of the inherent contradictions of the requirements for security, anonymity, and secrecy within the context of the legal and technical policies of the election process.

Acknowledgements

An earlier version of this paper [10] was posted online by the Center for Election Excellence and the American Bar Association shortly before the November 2008 general election in the United States for the explicit purpose of assisting election officials, candidates, and others in trying to coping with issues that arose. The authors of this paper wish to thank the reviewers who offered comments on the previous version of this paper, all of which which substantially aided this current version. Those reviewers included: Wayne Beckham, Charisse Castanoli, Cindy Cohn, David Dill, John Eichhorst, Jeremy Epstein, Sean Gallagher, Paul Hultin, Doug Jones, David Klein, Michael Losavio, Lelsey Mara, Peter McLennon, Larry Norden, Freddie Oakley, Marian K. Schneider, Fred Chris Smith, and Alec Yasinsac.

We also wish to thanks research assistants Timothy Ryan and Pleurat Dreshaj for their contributions to this paper.

Matt Bishop was supported in part by the National Science Foundation under Grant Number CNS-0716827.

Candice Hoke's work for the October 2008 version of this paper was partially supported by a consortium of national foundations seeking the adoption of best practices in election administration, including the Carnegie Corporation of New York, Democracy Alliance, Open Society Institute, Quixote Foundation, Rockefeller Brothers Fund, Working Assets, and other foundations via a grant to the Center for Election Excellence.

Sean Peisert was supported in part by the National Science Foundation under Grant Number CNS-0831002 and also in part by grant 2006-CS-001-000001 from the U.S. Department of Homeland Security, under the auspices of the Institute for Information Infrastructure Protection &

I3P research program. The I3P is managed by Dartmouth College.

The opinions, findings, and conclusions contained in this document are those of the authors and should not be ascribed to and do not necessarily reflect the views of the funders of any author, or the institutions with which any author is affiliated.

References

[1] Ohio Rev. Code Ann. Section 3501.11(J). http://www.sos.state.oh.us/SOS/elections/Directives/2008%20Directives/2008-96.aspx.

[2] Restatement (Third) of Agency, Section 8.14, 2006.

[3] Collaborative Public Audit of the 2006 Cuyahoga County General Election, Appendix 16-17. http://www.electionexcellence.org/devel/docs/Reports/LWV/Report_ElectionAudits.pdf, April 19 2007.

[4] E. Barr, M. Bishop, and M. Gondree. Fixing the 2006 Federal Voting Standards. *Communications of the ACM (CACM)*, 50(3), March 2007.

[5] K. Biba. Integrity Considerations for Secure Computer Systems. Technical Report MTR-3153, MITRE Corporation, Bedford, MA, April 1977.

[6] M. Bishop. *Computer Security: Art and Science*. Addison-Wesley Professional, Boston, MA, 2003.

[7] M. Bishop. *UC Red Team Report of California Secretary of State Top-to-Bottom Voting Systems Review*, July 2007.

[8] M. Bishop, S. Engle, C. Gates, S. Peisert, and S. Whalen. We Have Met the Enemy and He is Us. In *Proceedings of the 2008 New Security Paradigms Workshop (NSPW)*, Lake Tahoe, CA, September 22–25, 2008.

[9] M. Bishop, S. Engle, C. Gates, S. Peisert, and S. Whalen. Case Studies of an Insider Framework. In *Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS), Cyber Security and Information Intelligence Research Minitrack*, Waikoloa, HI, Jan. 5–8, 2009.

[10] M. Bishop, M. Graff, C. Hoke, D. Jefferson, and S. Peisert. Resolving the Unexpected in Elections: Election Officials' Options. Distributed by the Center For Election Excellence and the American Bar Association, October 8, 2008.

[11] M. Bishop and D. Wagner. Risks of E-Voting. *Communications of the ACM*, 50(11):120, November 2008.

[12] M. Blaze. Is the E-Voting Honeymoon Over? http://www.crypto.com/blog/vote_fraud_in_kentucky/, March 23, 2009.

[13] M. Blaze, P. McDaniel, and G. Vigna *et al. EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*. Secretary of State of Ohio, December 7, 2007.

[14] M. R. Clarkson, S. Chong, and A. C. Myers. Civitas: A Secure Voting System. *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, May 2008.

[15] M. R. Clarkson, B. Hay, M. Inge, A. Shelat, D. Wagner, and A. Yasinsac. Software Review and Security Analysis of Scytl Remote Voting Software. Technical report, Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, Florida, September 2008 2008.

[16] A. Cordero and D. Wagner. Replayable Voting Machine Audit Logs. In *Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, pages 1–14, San Jose, CA, 2008.

[17] J. Gideon. ES&S Vote Machine Memory Card Failures Spread to Other States. http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1064&Itemid=51, March 17 2006.

[18] J. Gideon. Summit County Ohio Threatens Legal Action Against ES&S. http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1105&Itemid=51, March 22 2006.

[19] S. N. Goggin, M. D. Byrne, J. E. Gilbert, G. Rogers, and J. McClendon. Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems. In *Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, pages 1–7, San Jose, CA, 2008.

[20] F. Graves and C. Graves. Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial. *Criminal Justice*, 19(1), Spring 2004.

[21] C. Hoke, R. Adrine, and T. Hayes. Final Report of the Cuyahoga Election Review Panel. http://www.electionexcellence.org/documents/ohio/cuyahoga/CERP_Final_Report_20060720.pdf, July 20 2006.

[22] E. Lipton and I. Urbina. In 5-Year Effort, Scant Evidence of Vote Fraud. *New York Times*, April 12, 2007.

[23] D. Molnar, T. Kohno, N. Sastry, and D. Wagner. Tamper-evident, History-Independent, Subliminal-Free Data Structures on PROM Storage-or-How to Store Ballots on a Voting Machine. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 365–370, 2006.

[24] National Research Council of the National Academies. *Strengthening Forensic Science in the United States: A Path Forward*. National Academies Press, 2009.

[25] S. Peisert. Forensics for System Administrators. *;login:*, 30(4):34–42, August 2005.

[26] S. Peisert and M. Bishop. I'm a Scientist, Not a Philosopher! *IEEE Security and Privacy Magazine*, 5(4):48–51, July–August 2007.

[27] S. Peisert, M. Bishop, S. Karin, and K. Marzullo. Analysis of Computer Intrusions Using Sequences of Function Calls. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 4(2):137–150, April–June 2007.

[28] S. Peisert, M. Bishop, S. Karin, and K. Marzullo. Toward Models for Forensic Analysis. In *Proceedings of the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*, pages 3–15, Seattle, WA, April 2007.

[29] S. Peisert, M. Bishop, and K. Marzullo. Computer Forensics *In Forensis*. In *Proceedings of the Third International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE-SADFE)*, pages 102–122, Oakland, CA, May 22, 2008.

[30] S. Peisert, M. Bishop, and A. Yasinsac. Vote Selling, Voter Anonymity, and Forensic Logging of Electronic Voting Machines. In *Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS), Digital Forensics – Pedagogy and Foundational Research Activity Minitrack*, Waikoloa, HI, Jan. 5–8, 2009.

[31] S. P. Peisert. *A Model of Forensic Analysis Using Goal-Oriented Logging*. PhD thesis, Department of Computer Science and Engineering, University of California, San Diego, March 2007.

[32] RABA Innovative Solution Cell. Trusted Agent Report Diebold AccuVote-TS Voting System. Technical report, RABA Technologies LLC, Columbia, MD, January 2004.

[33] R. L. Rivest and J. P. Wack. On the Notion of "Software Independence" in Voting Systems. http://vote.nist.gov/SI-in-voting.pdf, July 2006.

[34] B. Schneier and J. Kelsey. Secure Audit Logs to Support Computer Forensics. *ACM Transactions on Information and System Security (TISSEC)*, 2(2):159–176, May 1999.

[35] D. Wagner, D. Jefferson, M. Bishop, C. Karlof, and N. Sastry. Security Analysis of the Diebold AccuBasic Interpreter. Technical report, Voting Systems Technology Assessment Advisory Board, Office of the Secretary of State of California, Sacramento, CA, February 2006.

[36] A. Yasinsac and M. Bishop. Of Paper Trails and Voter Receipts. In *Proceedings of the 2008 Hawaii International Conference on System Sciences*, January 2008.

[37] A. Yasinsac and M. Bishop. The Dynamics of Counting and Recounting Votes. *IEEE Security and Privacy Magazine*, 6(3):22–29, May/June 2008.

[38] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester. *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware: Final Report For the Florida Department of State*. Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, Florida, February 23, 2007.

[39] K.-P. Yee. *Building Reliable Voting Machine Software*. PhD thesis, University of California, Berkeley, 2007.

[40] D. Zagorodnov, K. Marzullo, L. Alvisi, and T. C. Bressoud. Engineering Fault-Tolerant TCP/IP Servers Using FT-TCP. In *Proceedings of the 2003 International Conference on Dependable Systems and Networks (DSN)*, 2003.

Appendix 1: Example of Nondisclosure Agreement in Voting Equipment Review

From the California Top-to-Bottom Review (2007), contract between the California Secretary of State and the University of California but terms largely negotiated by academic Principal Investigators found at:
http://www.sos.ca.gov/elections/voting_systems/ttbr/sos_uc_contract.pdf

Exhibit A, Section 11, page 10, relevant text:

> No confidential information, record or data identified as proprietary or confidential that is provided or accessed that directly pertains or exclusively relates to this voting system review shall be discussed, published, disclosed, transferred or otherwise communicated outside the scope of the voting system review. No confidential documents, files, papers, records, computer disks, or other tangible matters containing such proprietary or confidential data, files or records shall be removed from secured locations without express written permission of one of the Principal Investigators. These confidentiality restrictions shall apply only to material that is received from the State and identified in writing as confidential. The following information shall not be considered confidential information for the purposes of these restrictions: information that was already known to the receiving party, other than under an obligation of confidentiality, at the time of disclosure; or information that is now or hereafter becomes publicly known by other than a breach of the nondisclosure agreements associated with this project. These restrictions shall not be construed to prevent team members from conducting future research on voting systems, possibly including the ones examined in this review, after the completion of this project, so long as that research does not improperly use confidential information gained through this review. The Principal Investigator of each UC team shall be responsible for requiring all members of the UC team, and any other project participants, to execute acknowledgements that they have read, understood and agreed to abide by the terms and conditions of this Statement of Work. Such executed acknowledgement shall remain in effect for the duration of the project even in the event of resignation or termination of the UC team member or participant. Upon completion of the final report, all proprietary or confidential information, data, and documentation, original and copies, provided by the SOS to UC shall be returned promptly to the attention. . . Secretary of State
> . . .

Appendix 2: Partial List of Voting Systems Studies

This appendix lists the studies of voting systems that are known and available for public access. The components of the voting systems listed are taken from the reports; note that different reports may refer to the same system in slightly different ways. Further, generic equipment (such as generic memory cards and Ethernet cables and switches) is omitted, even when listed in the reports. Each entry has the name by which the report is commonly referred. When projects have multiple reports, only the lead report or reports are listed. All reports are available on the listed web pages. Several reports, including some forensic reviews in an election context, are listed at the end but not in reverse chronological order or in the format of the balance, as they were received as the paper was going to press.

2008: Op Bravo/Scytl

Report: M. Clarkson, B. Hay, M. Inge, A, Shelat, D. Wagner, and A. Yasinsac, "Software Review and Security Analysis of Scytl Remote Voting Software," Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Sep. 2008).
URL: http://doe.dos.state.fl.us/voting-systems/pdf/FinalReportSept19.pdf
Voting System:

- Pnyx.core ODBP 1.0 remote voting software

2007: Ohio EVEREST

Report: "Project EVEREST (Evaluation and Validation of Election-Related Equipment, Standards, and Testing) Risk Assessment Study of Ohio Voting Systems: Executive Report," Office of the Secretary of State of Ohio, Columbus, OH (Dec. 2007). Additional reports available from teams based on vendor assignment.
URL: http://www.sos.state.oh.us/SOS/elections/voterInformation/equipment/VotingSystemReviewFindings.aspx
Voting Systems:

- Premier, consisting of:
  - GEMS software version 1.18.24

  - AccuVote-TSX version 4.6.4
  - AccuVote-OS 2000 Precinct Optical Scanner version 1.96.6
  - AccuVote-OS Central Optical Scanner version 2.0.12
  - Digi Seriel to Ethernet Gateway version PortServer II
  - VC Programmer ST100
  - Mobile Electronic Poll Worker Tablet System
  - Elections Media Processor System with Elections Media Drive Tower
  - Voter Card Encoder Spyrus PAR2
- ES&S, consisting of:
  - Unity Election Management Software version 3.0.1.1
  - Automark 87000
  - iVotronic DRE 90998-BI, 91057-BL, 93038-BL
  - Precinct Optical Scanner Model 100
  - Central Optical Scanner Model 650
- Hart Intercivic, consisting of:
  - BOSS, as provided by the Secretary of State
  - Tally, as provided by the Secretary of State
  - Rally, as provided by the Secretary of State
  - Servo, as provided by the Secretary of State
  - Trans, as provided by the Secretary of State
  - Ballot on Demand, as provided by the Secretary of State
  - eCM Manager, as provided by the Secretary of State
  - eCM Token, as provided by the Secretary of State
  - JBC
  - eSlate 3000 DRE version 4.0.1.9
  - eScan Optical Scanner version 1.1.6

2007: Florida Diebold Supplemental Report, SAIT Lab

Report: D. Gainey, M. Gerke, and A. Yasinsac, "Software Review and Security Analysis of the Diebold Voting Machine Software: Supplemental Report", Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Aug. 2007).
URL: `http://doe.dos.state.fl.us/voting-systems/pdf/dieboldRepriseRep.pdf`
Voting Systems:

- Diebold Voting System Software version 1.96.8

2007: Florida Diebold Report, SAIT Lab

Report: R. Gardner, A. Yasinsac, M. Bishop, T. Kohno, Z. Hartley, J. Kerski, D. Gainey, R. Walega, E. Hollander, and M. Gerke, "Software Review and Security Analysis of the Diebold Voting Machine Software", Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (July 2007).
URL: `http://doe.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf`
Voting Systems:

- Diebold Optical Scan firmware version 1.96.8
- Diebold Touch Screen firmware version 4.6.5
- Diebold Touch Screen bootloader version 1.3.6
- Diebold GEMS software version 1.18.25

2007: California Top to Bottom Review, University of California

Reports: M. Bishop, "Overview of Red Team Reports," Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (July 2007); D. Wagner, "Principal Investigator's Statement on Protection of Security-Sensitive Information," Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (Aug. 2007); and additional reports by vendor assignment by teams focused on Source Code, Red Team, Documentation Reviews. An omnibus Accessibility report is available rather than vendor-specific individual reports.
URL: `http://www.sos.ca.gov/elections/elections_vsr.htm`
Voting Systems:

- Diebold GEMS 1.18.24/AccuVote, consisting of:
  - GEMS software version 1.18.24
  - AccuVote-TSX with AccuView Printer Module and Ballot Station firmware version 4.6.4
  - AccuVote-OS (Model D) with firmware version 1.96.6
  - AccuVote-OS Central Count with firmware version 2.0.12
  - AccuFeed
  - Vote Card Encoder version 1.3.2

  - Key Card Tool software version 4.6.1
  - VC Programmer software version 4.6.1
- Hart Intercivic System 6.2.1, consisting of:
  - Ballot Now software version 3.3.11
  - BOSS software version 4.3.13
  - Rally software version 2.3.7
  - Tally software version 4.3.10
  - SERVO version 4.2.10
  - JBC version 4.3.1
  - eSlate/DAU version 4.2.13
  - eScan version 1.3.14
  - VBO version 1.8.3
  - eCM Manager, version 1.1.7
- Sequoia WinEDS version 3.1.012/Edge/Insight/400-C, consisting of:
  - WinEDS version 3.1.012
  - AVC Edge Model I firmware version 5.0.24
  - AVC Edge Model II firmware version 5.0.24
  - VeriVote Printer
  - Optech 400-C/WinETP firmware version 1.12.4
  - Optech Insight APX K2.10, HPX K1.42
  - Optech Insight Plus APX K2.10, HPX K1.42
  - Card Activator version 5.0.21
  - HAAT Model 50 version 1.0.69L
  - Memory Pack Reader (MPR) firmware version 2.15

2007: Center for Election Integrity, Cleveland State University

Report: Thomas P. Ryan and Candice Hoke, Cleveland State University GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards
URL: `http://www.usenix.org/events/evt07/tech/full_papers/ryan/ryan_html/`
Voting System: Diebold GEMS software

2007: Kentucky Attorney General

Report: J. Epstein, Security Consultant
URL: `http://www.eac.gov/program-areas/research-resources-and-reports/copy_of_docs/state-local-voting-system-reports`
Voting System:

- Hart Intercivic eSlate Voting System, software version 6.2.1 and related components
- Diebold Election Systems, Inc. AccuVote Optical Scan ("0s") (model D) with firmware version 1.96.6, Voter Card Encoder 1.3.2, AccuVote-OS Central Count firmware version 2.0.12, Key Card Tool 4.6.1, and VCProgrammer 4.6.1
- AccuVote-TSX DRE (Model D) Touch Screen with Ballot Station firmware version 4.6.4

2007: University of Connecticut VoTeR Report

Report: A, Kiayias, L. Michel, A. Russell, and A. Shvartsman, "Integrity Vulnerabilities in the Diebold TSX Voting Terminal," VoTeR Center, University of Connecticut, Storrs, CT 06269 (July 2007).
URL: `http://voter.engr.uconn.edu/voter/Report-TSX_files/TSXVoting_Terminal_Report.pdf`
Voting System:

- Diebold AccuVote-TSx firmware version 4.6.4, bootloader version BLR7-1.2.1, Windows CE Operating System version WCER-410.2.1
- Diebold GEMS server version 1.18

2006: University of California Hart Report

Report: E. Proebstel, S. Riddle, F. Hsu, J. Cummins, F. Oakley, T. Stanionis, and M. Bishop, "An Analysis of the Hart Intercivic DAU eSlate," Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (Aug. 2007).
URL: `http://www.usenix.org/events/evt07/tech/full_papers/proebstel/proebstel.pdf`
Voting System:

- Hart Intercivic eSlate version 6.1, consisting of:
  - eSlate firmware version 4.1.3
  - JBC firmware version 4.1.3
  - VBO firmware version 1.7.5

2007: Florida CD-13 (SAIT Report)

Report: A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware," Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL 32306-4530 (Feb. 2007).

URL: http://election.dos.state.fl.us/reports/pdf/FinalAudRepSAIT.pdf
Voting System:

- ES&S iVotronic firmware version8.0.1.2

2006: Diebold AccuBasic

Report: D. Wagner, D. Jefferson, M. Bishop, C. Karlof, and N. Sastry, "Security Analysis of the Diebold AccuBasic Interpreter," Technical Report, Voting Systems Technology Assessment Advisory Board, Office of the Secretary of State of California, Sacramento, CA 95814 (Feb. 2006).
URL: http://www.sos.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf
Voting Systems:

- Diebold AccuVote-OS with firmware version 1.96.6
- Diebold AccuVote-TSx with firmware version 4.6.4

2004: RABA Report

Report: RABA Innovative Solution Cell, "Trusted Agent Report Diebold AccuVote-TS Voting System," RABA Technologies LLC, Columbia, MD 21045 (Jan. 2004).
URL: http://nob.cs.ucdavis.edu/bishop/notes/2004-RABA/2004-RABA.pdf
Voting Systems:

- Diebold AccuVote-TS Voting System
- Diebold GEMS server

2003: Compuware Report

Report: "Direct Recording Electronic (DRE) Technical Security Assessment Report," Compuware Corporation, Columbus, OH 43229 (Nov. 2003).
URL: http://www.sos.state.oh.us/sos/upload/everest/01-compuware112103.pdf
Voting Systems:

- Diebold Election Systems, consisting of:
  - AccuVote-TS R6 firmware version 4.3.15
  - GEMS server version 1.18.18
- ES&S, consisting of:
  - iVotronic version 7.4.5.0
  - Unity Election System software version 2.2
- Hart InterCivic, consisting of:
  - eSlate 3000 version 2.1
  - JBC version 1.16
  - BOSS Election Management Software version 2.9.04
  - TALLY software version 2.9.08
  - SERVO software version 1.0.2
- Sequoia Voting Systems, consisting of:
  - AVC Edge version 4.1.D
  - Card Activator version 4.2
  - WinEDS Election Management Software version 2.6

Additional Reviews (with thanks to Prof. Doug Jones of the University of Iowa; this information will be organized for the next edition of this paper)

A forensics examination report for central-count mark-sense tabulators in Maricopa County, Arizona:
http://www.cs.uiowa.edu/~jones/voting/ArizonaDist20.pdf

A report on pre-election testing in Miami Dade County, Florida, with sections on central-count mark-sense tabulators and touch-screen machines, as well as general remarks on test design.
http://www.cs.uiowa.edu/~jones/voting/miamitest.pdf

Auditing elections – a discussion of how to do sanity checks on election results and pin down discrepancies. Forensic auditing clearly wants this, although I was more interested in on-the-fly self-auditing during the process.
http://www.cs.uiowa.edu/~jones/voting/cacm2004.shtml

Developing a Methodology for Observing Electronic Voting, a report from the Carter Center, includes Prof. Jones' talk on perspectives on electronic voting. This provides a framework for thinking about not only observing (the Carter Center's interest) but also forensic investigation. Forensic investigators will want the answers to essentially all the questions on the Carter Center's work sheets. http://www.cartercenter.org/documents/elec_voting_oct11_07.pdf (Republished in extended form in From Power Outages to Paper Trails, IFES).