Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records

To increase public confidence, states are increasingly considering electronic voting systems that provide voter-verified paper records. An analysis and evaluation of New Jersey's criteria against several different e-voting machine types revealed potential threats—and possible solutions—on privacy, security, and performance issues.

Nirwan Ansari, Pitipatana Sakarindr, Ehsan Haghani, Chao Zhang, Aridaman K. Jain, and Yun Q. Shi
New Jersey Institute of Technology

Governments around the world are increasingly replacing traditional paper ballots and punch cards with electronic voting systems such as the now 20-year-old direct-record electronic (DRE) system.[1] In such electronic voting (e-voting) systems, vendor-specific software controls system functionality, records and counts electronic votes, and generates the final results. Although e-voting systems are subject to federal and state certification, election officials and public advocates have raised many questions about their privacy, security, and performance. Before certifying a system, election officials must evaluate its hardware and software performance and its source code. However, simple lab testing is inadequate for detecting errors at all levels,[1,2] and undetected flaws can have devastating consequences in elections. Furthermore, weak requirements are fundamentally inefficient for ensuring voting system performance and security.[3] Thus, each state must examine and evaluate its own requirements to ensure the voting system's functionality, security, durability, and accessibility,[4] as well as the voting results' secrecy, privacy, and accuracy.

To increase voter confidence, some states have proposed—and in some cases, mandated—the addition of printers to voting machines.[4-5] This lets voters verify their voting selections on paper records; officials then couple the electronic record of each vote with a printed paper record. Using DREs with voter-verified paper-record systems (VVPRSs) should instill full public confidence in the electoral process. To certify such a system, however, analysts must carefully evaluate a printer's performance and its integration with the overall voting system.

Federal and state election commissions have made different recommendations for evaluating and certifying e-voting systems.[4-8] In the US, states have developed different requirements that target their particular needs. The Attorney General's Office of New Jersey issued criteria for e-voting machines equipped with printers[4] and asked the New Jersey Institute of Technology to test the various systems against these criteria.[9-12] As we discuss here, in the testing and analysis process, we encountered several issues of concern and formulated recommendations for addressing some of them.

System requirements

A DRE voting machine with VVPRS capability includes a ballot display unit, a voting panel, internal and external memories, a printer, a paper-record display unit, and a paper-record storage unit. The voting systems we tested all use thermal printers and adopt one of two methods: In *cut-and-drop* VVPRS, the individual printed paper records are cut and dropped into a storage unit; in *continuous spool* VVPRS, the vote selections are printed on a paper roll that rolls continuously from one spool to another.

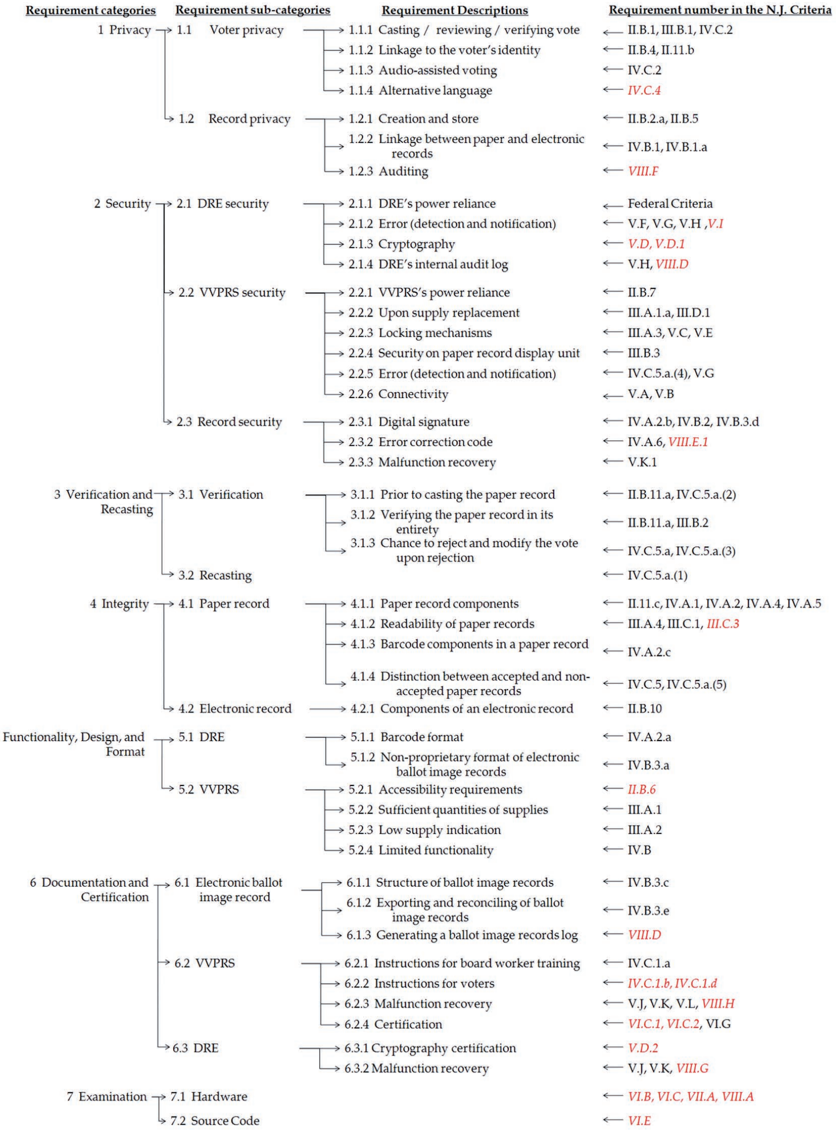
As Figure 1 shows, New Jersey's criteria define the system's component functionalities.

Privacy requirements

Voter privacy requirements are as follows:

- Voters must be able to privately and independently select candidates on the DRE machine and verify their selections on the printed paper record.
- The voter's identity can't be recorded or identified in the electronic and paper records, in the method that creates and stores these records, or in the method linking the DRE electronic-ballot-image record to the corresponding paper record.
- These same privacy protections must exist for visually impaired voters using audio-assistance.

Further, the electronic and paper records must be created, stored, and audited in a way that preserves their privacy.



Requirement categories	Requirement sub-categories	Requirement Descriptions	Requirement number in the N.J. Criteria
1 Privacy	1.1 Voter privacy	1.1.1 Casting / reviewing / verifying vote	II.B.1, III.B.1, IV.C.2
		1.1.2 Linkage to the voter's identity	II.B.4, II.11.b
		1.1.3 Audio-assisted voting	IV.C.2
		1.1.4 Alternative language	*IV.C.4*
	1.2 Record privacy	1.2.1 Creation and store	II.B.2.a, II.B.5
		1.2.2 Linkage between paper and electronic records	IV.B.1, IV.B.1.a
		1.2.3 Auditing	*VIII.F*
2 Security	2.1 DRE security	2.1.1 DRE's power reliance	Federal Criteria
		2.1.2 Error (detection and notification)	V.F, V.G, V.H ,*V.I*
		2.1.3 Cryptography	*V.D, V.D.1*
		2.1.4 DRE's internal audit log	V.H, *VIII.D*
	2.2 VVPRS security	2.2.1 VVPRS's power reliance	II.B.7
		2.2.2 Upon supply replacement	III.A.1.a, III.D.1
		2.2.3 Locking mechanisms	III.A.3, V.C, V.E
		2.2.4 Security on paper record display unit	III.B.3
		2.2.5 Error (detection and notification)	IV.C.5.a.(4), V.G
		2.2.6 Connectivity	V.A, V.B
	2.3 Record security	2.3.1 Digital signature	IV.A.2.b, IV.B.2, IV.B.3.d
		2.3.2 Error correction code	IV.A.6, *VIII.E.1*
		2.3.3 Malfunction recovery	V.K.1
3 Verification and Recasting	3.1 Verification	3.1.1 Prior to casting the paper record	II.B.11.a, IV.C.5.a.(2)
		3.1.2 Verifying the paper record in its entirety	II.B.11.a, III.B.2
		3.1.3 Chance to reject and modify the vote upon rejection	IV.C.5.a, IV.C.5.a.(3)
	3.2 Recasting		IV.C.5.a.(1)
4 Integrity	4.1 Paper record	4.1.1 Paper record components	II.11.c, IV.A.1, IV.A.2, IV.A.4, IV.A.5
		4.1.2 Readability of paper records	III.A.4, III.C.1, *III.C.3*
		4.1.3 Barcode components in a paper record	IV.A.2.c
		4.1.4 Distinction between accepted and non-accepted paper records	IV.C.5, IV.C.5.a.(5)
	4.2 Electronic record	4.2.1 Components of an electronic record	II.B.10
5 Functionality, Design, and Format	5.1 DRE	5.1.1 Barcode format	IV.A.2.a
		5.1.2 Non-proprietary format of electronic ballot image records	IV.B.3.a
	5.2 VVPRS	5.2.1 Accessibility requirements	*II.B.6*
		5.2.2 Sufficient quantities of supplies	III.A.1
		5.2.3 Low supply indication	III.A.2
		5.2.4 Limited functionality	IV.B
6 Documentation and Certification	6.1 Electronic ballot image record	6.1.1 Structure of ballot image records	IV.B.3.c
		6.1.2 Exporting and reconciling of ballot image records	IV.B.3.e
		6.1.3 Generating a ballot image records log	*VIII.D*
	6.2 VVPRS	6.2.1 Instructions for board worker training	IV.C.1.a
		6.2.2 Instructions for voters	*IV.C.1.b, IV.C.1.d*
		6.2.3 Malfunction recovery	V.J, V.K, V.L, *VIII.H*
		6.2.4 Certification	*VI.C.1, VI.C.2*, VI.G
	6.3 DRE	6.3.1 Cryptography certification	*V.D.2*
		6.3.2 Malfunction recovery	V.J, V.K, *VIII.G*
7 Examination	7.1 Hardware		*VI.B, VI.C, VII.A, VIII.A*
	7.2 Source Code		*VI.E*

Figure 1. Evaluation criteria derived from the New Jersey Attorney General's Office criteria for direct-record electronic (DRE) machines with voter-verified paper record systems (VVPRS). The requirements in red italics weren't part of the testing team's contract and therefore weren't tested.

Security requirements

Security requirements exist for the DRE System, the VVPRS, and for the vote records.

DRE system security. The voting system must prevent tampering with the election, the voting results, and the system's functionality. The voting system must withstand power-source failure and use a reserve battery to avoid poll closure. The DRE must detect any error or malfunction, report it to the election official and to the voter, and correctly record any such incident in the internal audit log. Finally, the US cryptographic module validation program must test and approve all voting system cryptographic software.[4]

VVPRS system security. The VVPRS must draw power from the DRE system or from the same circuit the DRE system uses to draw its power. Security features must be available for maintaining VVPRS integrity; for example, VVPRS printer components and the DRE-VVPRS connections must be secure. The VVPRS must be able to detect any error or malfunction and report it to the election official and the voter. The VVPRS must not be able to communicate externally to any system other than the DRE system. If any supply replacement is required, it must not circumvent the security features that protect the paper records' secrecy.

Vote record security. The voting systems can protect the vote record (that is, the paper and electronic records) by using digital signatures, which identify and authenticate the vote records, and error-correcting codes, which can help detect barcode read errors. The vote record should be fully recoverable in the event of malfunction or tampering.

Verification requirements

Before casting a vote, voters must be able to review and verify their selections on the DRE system and the corresponding paper records. New Jersey's criteria let voters reject and recast the ballot up to two additional times. Official workers must also have the opportunity to compare the electronic and paper records after the election for audit and recount purposes. Therefore, the electronic and paper records must be linked through a unique identifier.

Integrity requirements

There are separate integrity requirements for the paper and electronic records. The paper record must include every contest the voter casts on the DRE system, including write-ins and undervotes. It must also identify the election, the election district, and the voting machine. Moreover, the paper record's contents must be machine readable (using barcodes, for example) in case a recount and audit is needed. As noted earlier, the paper record must contain error-correcting codes to detect read errors. Finally, election officials must be able to distinguish between an accepted and rejected paper record.

Electronic records must include all votes cast by the voter, including write-ins and undervotes. The electronic record can include some security identities, such as digital signatures for an individual record and for the election's entire set of electronic records.

Format, design, and functionality requirements

Developers must create a voting machine that works with minimum disruption on Election Day. The machine must be provisioned with a sufficient amount of voting supplies, such as paper and ink. If the DRE runs low on paper, it must let the current voter fully verify all of his or her vote selections and successfully cast the ballot without disruption before a paper replacement. Developers must design the VVPRS to function only as a printer; it must not be capable of networking or communicating externally with any system other than the DRE system. Finally, the electronic-ballot-image record's format must be publicly available and non-proprietary; in addition, the ballot's barcode must use an industry standard format and be readable with any commercial barcode reader.

Documentation and certification requirements

The vendor must supply documentation for election worker training, voting instructions, and malfunction recovery. The vendor must submit all federally certified Independent Testing Authority reports on the DRE with VVPRS.

Examination requirements

The VVPRS must be subject to the State Voting Machine Examination Committee's scrutiny. In addition, the vendor must provide the state with the DRE and VVPRS source code for independent testing.

Testing techniques

We designed and conducted four testing approaches—a single test, a 1,200-vote simulated test, a 14-hour test, and a 52-vote test—to examine VVPRS against certain state requirements; for all, we used accepted scientific practices and methodologies. We recruited students with different backgrounds to act as "mock voters"; they ranged from undergraduates to PhD candidates. Mock voters cast votes in various voting scenarios, each of which represented particular selections of an election's contest positions. We printed the scenarios on cards, which the testing team shuffled to achieve randomization prior to giving them to the mock voters. Each voter made selections as indicated on each scenario card under the testing team's close supervision.

Ballots

We adopted two ballot types: one long, one short. As Figure 2 shows, the long ballot—which we used for the 14-hour and 52-vote tests—contained 19 items to vote on. We designed 12 voting scenarios to represent all possible choices, including eight party voting scenarios that were completely balanced (two parties for seven contests; seven "yes" or "no" questions; and 10 candidates listed for the charter study commission). In the eight voting scenarios, each position got four Democratic (D) and four Republican (R) candidate votes, and each question got four "yes" votes and four "no" votes. We also had four supplementary voting scenarios that we designed to test possibilities not included in the eight scenarios. Finally, we considered two additional cases from among the 12 scenarios to test whether voters could reject and recast their ballot during the 14-hour test. In the first case, voters voided their first set of selections (one of the 12 scenarios) and recast their votes for the second set (another of the 12 scenarios). In the second case, voters voided their first two sets of selections and recast their votes for the third and final selection.

We used a short ballot in the 1,200-vote test; this ballot featured the same 12 voting scenarios as the long ballot, but omitted the charter study commission and had few questions. The ballot contained eight party voting scenarios (again, completely balanced, with two parties for five positions, and "yes" or "no" votes for four questions) and four supplementary voting scenarios.

For all volume tests, we retained summaries of the following records:

- tabulation of final paper records,
- tabulation of the final paper records' scanned barcodes,
- electronic records, and
- the closed poll's tally report.

Each summary gave the vote counts for each contest candidate (including the questions).

LONG BALLOT		MAJOR PARTY SCENARIO NUMBER								SUPPLEMENTARY SCENARIO NUMBER			
		1	2	3	4	5	6	7	8	9	10	11	12
Position	PRES	R	D	D	D	D	R	R	R	PET1	PET2		WRITE-IN
	US-S	D	R	D	D	R	R	R	D	WRITE-IN		WRITE-IN	
	US-H	R	R	D	R	D	R	D	D	WRITE-IN		WRITE-IN	
	F 3-YR-1	R	R	D	D	R	D	D	R	WRITE-IN		WRITE-IN	
	F 3-YR-2	D	R	D	R	D	D	R	R		WRITE-IN	WRITE-IN	
	F 2-YR	R	D	D	R	R	D	R	D	WRITE-IN		WRITE-IN	
	TOWNSHIP	D	D	D	R	R	R	D	R	WRITE-IN		WRITE-IN	
Question	1	NO	YES	NO	NO	YES	YES	NO	YES				
	2	NO	NO	YES	NO	NO	YES	YES	YES				
	3	NO	YES	NO	YES	NO	YES	YES	NO				
	4	NO	YES	YES	NO	YES	NO	YES	NO				
	5	NO	NO	NO	YES	YES	NO	YES	YES				
	6	NO	YES	YES	YES	NO	NO	NO	YES				
	7	NO	NO	YES	YES	YES	YES	NO	NO				
Charter study commission	1	N1	N6	N1	N4	N10		N6	N8	N1	N6	N9	
	2	N2	N7	N2	N5	W1		N7	N9	N2	N7	N10	
	3	N3	N8	N3		W2		W3	N10	N3	N8		
	4	N4	N9							N4			
	5	N5								N5			
No. of charter study commission voted		5	4	3	2	3	0	3	3	5	3	2	0

Figure 2. The long ballot. The 12 voting scenarios—eight major party and four supplementary—represent all possible choices. "R" and "D" stand for a vote for a Republican or Democratic name, respectively. A blank space indicates a "no" vote for that position. For the charter study commission, N1, N2, …, N10 indicate a vote for Name1, Name2,…, Name 10, respectively. W1, W2, and W3 are the three write-in names for the charter study commission.

Single test

In the single test, we ran a one-time examination of specific criteria using different testing methods. For example, the test might be a physical inspection of various DRE and VVPRS components. In many cases, we retrieved, studied, and compared paper records, electronic records, and barcodes. For example, we verified deployment of error-correction codes and digital signatures by closely examining these records. In some cases, we forced incidental and procedural hindrances—such as a paper jam—to observe the effect. We also closely examined all vendor documentations.

14-hour test

Our 14-hour test emulated actual physical voting situations over a 14-hour period (representing an entire election day). Each mock voter cast votes over a one- to two-hour time slot using the long ballot. We gave each mock voter a set of shuffled scenario cards derived from eight sets of eight major party voting scenarios and one set of four supplementary voting scenarios. We also randomly inserted questionnaire cards that asked voters questions about the voting scenario.

1,200-vote simulated test

The state's criteria recommends that each machine be capable of processing 750 ballots; we designed this test to investigate the voting system's response to a larger than expected number of ballots, which tend to overload the system's capability. Using a short ballot and a scripted program, we ran a simulated test in which each machine continuously generated 1,200 votes. To reach the 1,200 vote total, the test generated each of the eight party-voting scenarios 125 times, and each of the four supplementary voting scenarios 50 times.

Table 1. Configurations of the four machine types.

COMPONENTS	MACHINE TYPE 1	MACHINE TYPE 2	MACHINE TYPE 3	MACHINE TYPE 4
DRE SYSTEM				
User interface	32″ LCD touch screen	A panel with matrix-liked switch buttons and a write-in LCD screen and keyboard	15″ LCD touch screen	15″ LCD touch screen
Ballot-activation device	An RFID smart card with a card encoder	An activation button on an official panel	An RFID smart card with a card encoder and a button at the back of the DRE	An Infrared Data Association (IrDA) proprietary device with an encoding cradle
Electronic-record storage device	Built-in memory, flash drive, DVD	Built-in memories, a proprietary device designed by Personal Computer Memory Card International Association (PCMCIA)	Built-in memories, a proprietary PCMCIA device	Three built-in memories; a compact flash card; a proprietary, IrDA-designed device
Audio-assisted voting interface	A modified keyboard with four different button shapes and a headset	A proprietary four-button panel and a headset	A proprietary four-button panel and a headset	Four buttons with different shapes on the DRE and a headset
Magnification device?	Yes	Yes	Yes	Yes
Externally connected printer?	No	Yes (an additional printer and a VVPRS printer simultaneously connected to the DRE)	No	Yes (an additional printer and a VVPRS printer connected to the DRE one at a time)
Power source	Primarily alternating current (AC), with a battery backup (up to 16 hours, with a maximum of four battery packs)	Primarily AC, with a battery backup (up to 16 hours)	Primarily AC, with a battery backup (up to two hours)	Primarily AC, with a battery backup (up to two hours)
Power daisy chains	Yes (three AC outputs)	Yes (10 AC outputs)	Yes (one AC output)	Yes (six AC outputs)
Interfaces/adapters (observed)	2 Personal System/2 ports (PS/2 to USB adapter also provided); 4 USB ports; 1 IEEE 1284; 2 recommended standard ports (RS-232); 1 supervideo graphics array (SVGA); 1 registered jack (RJ-45); 1 Ethernet; 1 RFID slot; audio	1 IEEE-1284; 1 RJ-45; 2 PCMCIA slots	1 IEEE-1284; 1 RJ-45; 2 PCMCIA slots	1 RS-232; 1 IrDA slot; 1 compact Flash slot; audio
VVPRS COMPONENT				
Printer type	Cut-and-drop	Cut-and-drop	Continuous spool	Continuous spool
Paper type	Thermal	Thermal	Thermal	Thermal
Paper size (print width)	80 mm	80 mm	80 mm	80 mm
Paper-record storage unit	Metal box	Bag	Spool	Spool
Paper supply capacity (approximate)	600 votes	500 votes	120 votes	120 votes

In cases in which the machines lacked the script capability to automate this test, we had mock voters cast the 1,200 votes manually.

52-vote test

Finally, we designed a 52-vote test to investigate the special case in which the paper record extends to multiple pages. This criteria applies only to VVPRSs using the cut-and-drop method (in this case, machine types 1 and 2). We ran this test using the long ballot and mock voters.

Problems and criteria exceptions

We tested four machine types with different configurations from different manufacturers. Table 1 shows the machines' features; to maintain confidentiality, we don't disclose the vendors' identities, the machines' models and serial numbers, or other proprietary information. As Table 2 summarizes, the systems didn't comply with all of the state's criteria during our tests. The problems and criteria exceptions fell into several general categories as follows.

Voter privacy

We found several violations of the state's requirements for voter privacy (Figure 1, subcategory 1.1). First, regarding vote casting, reviewing, and verifying, machine types 2, 3, and 4 offered physical enclosures—including two-sided panels, a top panel, and a curtain—but failed to provide full voter privacy. Observers placed around the voting machine were able to read vote selections on the DRE screen and on the paper record in its display unit. Although sneaking inside or loitering around poll booths is illegal in real elections, these machine types still pose a privacy threat to voters. To mitigate such a threat, these machines must be strategically placed, such as facing outward from a wall.

Second, the machines had problems regarding protecting links between votes and voter identities. One machine (type 4) printed the paper record with the exact voting date and time. Comparing this timestamp to the poll log (which records the voter's check-in time) could match the paper record to the voter and thus reveal his or her identity.

Finally, we encountered privacy issues when we tested audio-assisted voting on a type 2 machine. In this case, the cut-and-drop printer printed the paper record in multiple pages. After printing the first paper-record page, the system displayed a message on the DRE screen rather than providing an audio message. The displayed message prompted the voter to press a button on the DRE to print the next page; pressing the button on an audio-assisted voting panel produced no results. Assuming audio-assisted voters are visually impaired, they're unlikely to see the message displayed on the DRE screen. Consequently, they'd likely seek assistance from a poll worker, who might see vote selections (displayed on the DRE screen and in the paper-record display unit), thus violating visually impaired voters' privacy.

Record privacy

We found several violations of the state's paper and electronic record privacy requirements (Figure 1, subcategory 1.2). First, regarding the creation and store requirements, the type 4 machine recorded the electronic record when voters approved their ballots on the DRE screen, rather than after they approved the paper record.

Second, regarding the linkage between paper and electronic records, the machines did use a unique identifier to link the two records. However, in machine types 3 and 4, the reconciliation process was time consuming and difficult given a large vote volume. With the type 2 machine, it would likely be impossible to reconcile the two records if one or more paper records were lost.

DRE security mechanisms

We encountered several problems with DRE security mechanisms (Figure 1, subcategory 2.1). Regarding error detection and notification, machine type 1's DRE didn't suspend voting when the printer cable was disconnected. It also failed to emit any signal to the election official. Although the DRE recorded the vote electronically, the VVPRS didn't print the paper record. Machine type 2's DRE displayed an error notification when a mechanical error or malfunction occurred, but the error message didn't always reflect the actual problem. Also, the DREs of types 3 and 4 couldn't detect a paper jam. Regarding internal audit log criteria, when the printer cable between the DRE and VVPRS was disconnected, the type 2 and 3 machines' DREs didn't record the incident.

VVPRS security mechanisms

We found three violations in this category (Figure 1, subcategory 2.2). First, regarding supply replacement security, when we restocked the paper supply, type 3 and 4 machines didn't have sufficient security locks to protect the paper records in the paper-record storage unit. More important, in machine type 1, there was a slit in the paper-record storage unit, through which corrupt election officials could slide fraudulent paper records after they'd unlocked the printer cover to restock the paper supply.

Second, regarding locking mechanisms, machine types 1, 3, and 4 publicly exposed part of the printer cable, which could be tampered with to disrupt functions during the election. Machine type 2 had no locking mechanism for the printer cover.

Table 2. Problems found in four tested machine types.

CATEGORY	CRITERIA	PROBLEMS/CRITERIA EXCEPTIONS	MACHINE TYPE 1	MACHINE TYPE 2	MACHINE TYPE 3	MACHINE TYPE 4
1.1.1	II.B.1, III.B.1, IV.C.2	Voter privacy (casting/reviewing/verifying)	✓	✗	✗	✗
1.1.2	II.B.4, II.11.b	Voter privacy (linkage)	✓	✓	✓	✗
1.1.3	IV.C.2	Voter privacy (audio-assisted voting)	✓	✗	✓	✗
1.1.4	*IV.C.4*	Voter privacy (alternative language)	*Not tested*	*Not tested*	*Not tested*	*Not tested*
1.2.1	II.B.5, II.B.2.a	Record privacy (creation and storage)	✓	✓	✓	✗
1.2.2	IV.B.1, IV.B.1.a	Linkage between paper and electronic records	✓	✗	✗	✗
1.2.3	*VIII.F*	Record privacy (auditing)	*Not tested*	*Not tested*	*Not tested*	*Not tested*
2.1.1	Federal criteria	DRE's power reliance	Battery reserves, up to 16 hours	Battery reserves, up to 16 hours	Battery reserves, up to two hours	Battery reserves, up to 12 hours
2.1.2	V.F, V.G, V.H, *V.I*	DRE's error detection and notification	✗	✗	✗	✗
2.1.3	*V.D, V.D.1*	Cryptography	*Not tested*	*Not tested*	*Not tested*	*Not tested*
2.1.4	V.H, *VIII.D*	DRE's internal audit log	✓	✗	✗	✓
2.2.1	II.B.7	VVPRS's power reliance	✓	✓	✓	✓
2.2.2	III.A.1.a, III.D.1	VVPRS security upon supply replacements	✗	✓	✗	✗
2.2.3	III.A.3, V.C, V.E	VVPRS's locking mechanisms	✗	✗	✗	✗
2.2.4	III.B.3	Paper record display unit	✓	✓	✓	✓
2.2.5	IV.C.5.a.(4) , V.G	VVPRS's error detection and notification	✗	✓	✗	✗
2.2.6	V.A, V.B	VVPRS's connectivity	✓	✓	✓	✓
2.3.1	IV.A.2.b, IV.B.2, IV.B.3.d	Digital signature	✗	✗	✗	✗
2.3.2	IV.A.6, *VIII.E.1*	Error correction code	✓	✓	✓	✓
2.3.3	V.K.1	Malfunction recovery for records	✓	✓	✓	✓
3.1.1	II.B.11.a, IV.C.5.a.(2)	Verification (prior to casting)	✓	✗	✗	✗
3.1.2	II.B.11.a, III.B.2	Verification (of entire paper record)	✓	✓	✓	✗
3.1.3	IV.C.5.a, IV.C.5.a.(3)	Verification (chance to reject/ modify upon rejection)	✓	✓	✓	✗
3.2	IV.C.5.a.(1)	Recasting	✓	✓	✓	✗
4.1.1	II.11.c, IV.A.1, IV.A.2, IV.A.4, IV.A.5	Paper record components	✗	✗	✓	✓
4.1.2	III.A.4, III.C.1, *III.C.3*	Readability of paper records	✓	✓	✓	✗
4.1.3	IV.A.2.c	Barcode components in a paper record	✓	✓	✓	✓
4.1.4	IV.C.5, IV.C.5.a.(5)	Distinction among accepted and unaccepted paper records	✗	✓	✓	✗
4.2.1	II.B.10	Components of electrical record	✓	✓	✓	✓
5.1.1	IV.A.2.a	DRE's barcode format	✓	✓	✓	✓
5.1.2	IV.B.3.a	Nonproprietary format of the DRE's electronic ballot image records	✓	✓	✓	✓
5.2.1	*II.B.6*	VVPRS's accessibility	*Not tested*	*Not tested*	*Not tested*	*Not tested*
5.2.2	III.A.1	VVPRS's sufficient quantities of supplies	✗	✗	✗	✗
5.2.3	III.A.2	VVPRS's low supply indication	✗	✓	✓	✗
5.2.4	IV.B	VVPRS's limited functionality	✓	✓	✓	✓
6.1.1	IV.B.3.c	Documentation (structure of ballot image records)	✓	✓	✓	✓

Table 2. Problems found in four tested machine types.

CATEGORY	CRITERIA	PROBLEMS/CRITERIA EXCEPTIONS	MACHINE TYPE 1	MACHINE TYPE 2	MACHINE TYPE 3	MACHINE TYPE 4
6.1.2	IV.B.3.e	Documentation (exporting and reconciling ballot image records)	✓	✓	✓	✗
6.1.3	*VIII.D*	Documentation (generating a ballot image record log)	*Not tested*	*Not tested*	*Not tested*	*Not tested*
6.2.1	IV.C.1.a	Instructions for election worker training	✓	✓	✓	✓
6.2.2	*IV.C.1.b, IV.C.1.d*	Instructions for voters	*Not tested*	*Not tested*	*Not tested*	*Not tested*
6.2.3	V.J, V.K, V.L, *VIII.H*	Documentation (VVPRS malfunction recovery)	✓	✓	✓	✓
6.2.4	*VI.C.1, VI.C.2*, VI.G	Certification	✗	✗	✗	✓
6.3.1	*V.D.2*	Cryptographic certification	*Not tested*	*Not tested*	*Not tested*	*Not tested*
6.3.2	V.J, V.K, *VIII.G*	Documentation (DRE malfunction recovery)	✓	✓	✓	✓
7.1	*VI.B, VI.C, VII.A, VIII.A*	Hardware and software examination	*Tested VVPRS-related hardware only*	*Tested VVPRS-related hardware only*	*Tested VVPRS-related hardware only*	*Tested VVPRS-related hardware only*
7.2	*VI.E*	Source code examination	*Not tested*	*Not tested*	*Not tested*	*Not tested*

A check mark (✓) indicates no problems during testing; a cross mark (✗) indicates problems related to the criteria requirements. Criteria in red italics were not tested.

Third, regarding error detection and notification, when we disconnected the type 1 machine's printer cable, the VVPRS didn't send a signal to the official. The voter could continue voting and cast the vote, but the machine failed to print a paper record. With the type 3 machine, a VVPRS mechanical error or malfunction didn't prompt any error message or warning signal, it simply froze the system. Type 4's VVPRS couldn't detect a paper jam; the voter could cast votes, but the printer kept printing over the same area on the paper, making it illegible. Moreover, if the machine's printer cable was disconnected after the voter pressed the "cast vote" button, the machine recorded the electronic record, but didn't print a barcode on the paper record.

Vote record security mechanisms

All four machines violated vote record security requirements (Figure 1, subcategory 2.3) in relation to digital signatures. The type 1 machine generated electronic records' digital signatures based on the vendor's proprietary scheme, rather than on the required one-to-one scheme (that is, one digital signature for each electronic record). The type 2 and 3 machines also failed to generate individual digital signatures for each electronic record. Thus, all three machines calculated digital signatures for the entire set of electronic records using only the electronic records, not their corresponding digital signatures. The type 4 machine didn't generate a digital signature for individual electronic records or for the entire set of electronic records.

Paper-record verification

We found three violations of the requirements in this category (Figure 1, subcategory 3.1). First, after voters on type 2 and 3 machines rejected their first two paper records, the system wouldn't let them adequately verify their third paper record (although it printed, it displayed for only a few seconds before spooling). The type 4 machine printed only one paper record per voter; voters could review and verify subsequent ballots on the DRE screen, but not on the paper record. Once they cast their ballots, the machine printed the paper record, but it was rapidly advanced to the spool.

Second, the type 4 machine let voters review and modify each vote selection one-by-one an unlimited number of times. It also immediately printed each modification—that is, each selection, deselection, or change—line-by-line. However, it didn't print undervotes in the line-by-line printing, and thus voters couldn't verify undervotes on the paper record before casting.

Finally, the type 4 machine printed only one paper record per voter. Consequently, voters couldn't reject the paper record and then modify their ballots. This problem also violated the state's criteria for vote recasting and paper records (Figure 1, subcategory 3.2) because it didn't let voters recast their ballot up to two additional times.

Paper-record integrity

We found three violations in this category (Figure 1, subcategory 4.1). First, type 1 and 2 machines didn't print the election name on the paper record. Second, the type 4 machine's paper-record printout used a smaller font size than mandated by the criteria. Third, the type 1 machine didn't print clear acceptance information—that is, "voided" or "accepted"—on the paper record.

VVPRS component functionality, design, and format

We found one violation in this category (Figure 1, subcategory 5.2). When the type 1 machine detected a low paper supply, the DRE screen displayed an error message, and voters could continue voting and cast their ballots. However, the machine didn't print the paper record. This continued with subsequent voters, and the machine sent no audio or visual signal to the election official. To reset the voting system, we had to shut it down. In the type 4 machine, if the paper amount reached the minimum limit during a voting session, the DRE voided the ballot and didn't let the voter complete casting the vote.

Volume testing issues

We observed several paper jams in volume tests. During a 1,200-vote simulated test on the type 2 machine, a paper jam occurred and 56 paper records didn't print. The DRE continued to cast votes electronically without the VVPRS printing the paper records. Once the paper jam was cleared, the printing resumed. However, because the 56 paper records were lost, we couldn't reconcile the paper and electronic records, and thus it was impossible to conduct an audit. (This phenomenon wouldn't occur during an official election, as poll workers must activate the machine for each voter to cast his or her vote.) In the type 4 machine, a paper jam during the 14-hour test resulted in paper being torn apart, and selections and barcodes didn't print.

Suggestions and solutions

On the basis of our experience in this testing project, we propose some solutions to mitigate the identified problems. Election officials can implement some of these solutions using procedural and operational instructions; others require software/firmware changes.

Privacy

Election officials should issue procedural instructions for poll workers so they can strategically place vulnerable voting systems, and thus avoid privacy violations when people loiter near the booth. When mechanical errors or malfunctions occur that require official assistance, voter and ballot privacy must be maintained. To achieve this, developers can design voting systems such that voters can hide vote selections displayed on the DRE and in the paper-record display unit prior to seeking assistance. Also, for certain errors, the official could give the voter troubleshooting instructions while standing outside the booth.

Security

Election officials should be required to thoroughly examine and use physical locking and protective mechanisms. For example, states should require each polling place to establish a hierarchical access with respect to a custody chain. Also, developers should design the voting system to protect paper records with two or more security layers—one to secure the printer cover, and another to secure the storage unit.

To replace a paper supply, election workers should have a key that opens the printer cover and lets them restock the paper, but that key shouldn't open the lock protecting the paper-record storage unit. Each polling place should require two or more authorized supervisors to be present before officials can access paper records. To increase security, such officials might use different keys in escrow to open the storage unit's lock. Officials should secure the physical memory or cartridge that stores electronic records in the same way as the paper-record storage unit.

As we discussed earlier, states should mandate that the digital signature be generated both for each individual electronic record as well as for the entire election's set of electronic records. Further, the digital signature generation algorithm should adopt the latest standards, with proper algorithm parameters as recommended by the National Institute of Standards and Technology.

Other issues

There are three other issues that require clear mandates. First, regarding verification and recasting, voters must be able to take affirmative action—that is, press a "cast vote" button—to verify their third and final paper record, but they shouldn't be able to reject, modify, or recast that third paper record.

Second, accepted and rejected paper records must be clearly distinguishable—that is, they must be clearly marked "Voided" or "Accepted"—to prevent any confusion during a recount or audit.

Finally, electronic records are typically protected and must be extracted using the vendors' proprietary software. An independent testing agency must be able to evaluate this proprietary software to ensure the proper protection of electronic records. The agency should also rigorously evaluate all DRE system source codes to identify and reduce any code errors (bugs or vulnerable codes) as well as any malicious codes (such as backdoor codes).

It's fair to say that most of the machines we tested met most of the state's criteria. Still, our testing revealed several problems that must be addressed to instill public confidence in using DRE with VVPRS. Although our testing was applied only to voting systems subject to the State of New Jersey's approval, we believe that other states can apply and tailor our analysis, methodologies, testing scenarios, and solutions for their different requirements and needs. □

Acknowledgments

Our team members—Michell Darer, Dennis O'Brian, Chunhua Chen, and Caroline Christensen—contributed significantly to this project, and we appreciate their support.

References

1. J. Epstein, "Electronic Voting," *Computer*, vol. 40, no. 8, 2007, pp. 92–95.
2. T. Kohno et al., "Analysis of an Electronic Voting System," *Proc. IEEE Symp. Security and Privacy*, IEEE CS Press, 2004, pp. 27–40.
3. R.T. Mercuri, *Electronic Vote Tabulation Checks and Balances*, dissertation, Dept. of Computer and Information Systems, Univ. Pennsylvania, Oct. 2000.
4. New Jersey Division of Elections, *State of New Jersey Criteria for Voter-Verified Paper Record for Direct Recording Electronic Voting Machines*, April 2007; www.nj.gov/oag/elections/voter_issues/Final-VVPRS-Criteria.pdf.
5. US Election Assistance Commission, *2005 Voluntary Voting System Guidelines,* vol. I (version 1), 2005; www.eac.gov/voting%20systems/docs/vvsgvolumei.pdf.
6. US Election Assistance Commission, *2005 Voluntary Voting System Guidelines*, vol. II (version 1), 2005; www.eac.gov/voting%20systems/docs/vvsgvolume_ii.pdf.
7. U.S. Election Assistance Commission, *2007 Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission,* Aug. 2007; http://vote.nist.gov/VVSG-0807/Final-TGDC-VVSG-08312007.pdf.
8. California Division of Elections, *Top-to-Bottom Review Reports of the Voting System*, July 2007; www.sos.ca.gov/elections/voting_systems/ttbr/.
9. *Avante Vote-Trakker Voter-verified Paper Record Assessment*, report to NJ Attorney General, NJ Institute of Technology, 18 July 2007; www.nj.gov/oag/elections/Hearing-Reports-7.07/NJIT-Avante-report-7.07.pdf.
10. *Sequoia AVC Advantage Voter-verified Paper Record Assessment*, report to NJ Attorney General, NJ Institute of Technology, 18 July 2007; www.nj.gov/oag/elections/Hearing-Reports-7.07/NJIT-Advantage-report-7.07.pdf.
11. *Sequoia AVC Edge Voter-verified Paper Record Assessment*, report to NJ Attorney General, NJ Institute of Technology, 18 July 2007; www.nj.gov/oag/elections/Hearing-Reports-7.07/NJIT-Edge-report-7.07.pdf.
12. *Election Systems & Software iVotronic w/RTAL Voter-verified Paper Record Assessment*, report to NJ Attorney General, NJ Institute of Technology, 26 Sept. 2007; www.nj.gov/oag/elections/Hearing-Reports-7.07/ES&S_Final_Report_Sept%2026_2007.pdf.

***Nirwan Ansari** is professor in the Department of Electrical and Computer Engineering at the New Jersey Institute of Technology. His research interests include various aspects of broadband networks and multimedia communications. Ansari has a PhD in electrical engineering from Purdue University. Contact him at ansari@njit.edu.*

***Pitipatana Sakarindr** is a PhD candidate in the Department of Electrical and Computer Engineering at the New Jersey Institute of Technology. His research interests include network security, trust and reputation, secure group communications, and cryptography. Sakarindr has an MS in computer engineering from the New Jersey Institute of Technology. Contact him at ps6@njit.edu.*

***Ehsan Haghani** is a PhD candidate in the Department of Electrical and Computer Engineering at the New Jersey Institute of Technology. His research interests include various aspects of wireless networks including resource allocation and cross-layer design. Haghani has an MS in communications engineering from Chalmers University of Technology, Sweden. Contact him at ehsan@njit.edu.*

***Chao Zhang** is a PhD candidate in the Department of Electrical and Computer Engineering at the New Jersey Institute of Technology. His research interests include security in wireless networks, with an emphasis on ad hoc and sensor networks. Zhang has an MS in computer science from the New Jersey Institute of Technology, and an MS in physics from Fudan University, China. Contact him at Chao.Zhang@njit.edu.*

***Aridaman K. Jain** is senior university lecturer in the Division of Mathematical Sciences at the New Jersey Institute of Technology. His research interests include statistical modeling, sampling surveys, design of experiments, and data analysis. Jain has a PhD in statistics and industrial engineering from Purdue University. Contact him at jain@njit.edu.*

***Yun Q. Shi** is professor in the Department of Electrical and Computer Engineering at the New Jersey Institute of Technology. His research interests include watermarking, data hiding, steganalysis, forensics, and multimedia security. Shi has a PhD in electrical engineering from University of Pittsburgh. Contact him at Shi@njit.edu.*