Security in the Georgia Voting System

Britain J. Williams, Ph.D.

April 23, 2003

Introduction: The State of Georgia replaced all voting systems statewide with a computer-based voting system. This system, known as a direct recording electronic (DRE) voting system, was first used in the November 2002 election. This voting system, described in the next section, is computer based. As a result, questions have been raised regarding the vulnerability of the system to attacks by hackers and persons attempting election fraud.

Overall security of any computer-based system is obtained by a combination of three factors working in concert with each other. First, the computer system must provide audit data that is sufficient to track the sequence of events that occur on the system and, to the extent possible, identify the person(s) that initiated the events. Next, there must be in place well defined and strictly enforced policies and procedures that control who has access to the system, the circumstances under which they can access the system, and the functions that they are allowed to perform on the system. Finally, there must be in place physical security; fences, doors, locks, etc.; that control and limit access to the system. This article describes how these factors are incorporated into the election system in the State of Georgia.

Overview of the Georgia Voting System: The computer-based election system deployed in the State of Georgia is classified as a direct recording electronic (DRE) system. The components of the system consist of the following:

> Standard personal computers running an executable module known as GEMS, Global Election Management System. This system, called the GEMS computer, is used to define the election, enter the candidates and questions, and format the ballots for the voting devices. This computer also accumulates the votes after the polls close and prints various reports and audits.
>
> Touch-screen voting stations are used for in-person voting.
>
> Optical ballot scanners are used for absentee and provisional voting.

Each county election office in the State is equipped with a GEMS computer. This computer is used to define elections and format the ballots for both the touch-screen voting stations and the absentee (paper) ballot scanners. The system also produces files that can be sent directly to a printer to print the absentee and provisional ballots.

When the election definition is complete, the GEMS system produces PCMCIA cards, also called PC memory cards, which are used to program the touch-screen voting stations and the ballot scanners. One card is produced for each voting station and ballot scanner.

While still in the county warehouse the voting stations are arranged by precinct and the PC cards are inserted. In the days just before the election a series of tests called Logic and Accuracy tests are conducted. These tests are designed to confirm that the voting stations have been properly prepared for the election and that they correctly register all votes cast. These tests are open to the public. At the completion of the Logic and Accuracy tests the voting stations are sealed and delivered to the precincts.

On the morning of Election Day the Precinct Manager and Assistant Precinct Manager break the seals and prepare the voting stations for the election. The first step in this process is to print out a 'zero totals tape'. This tape verifies that no votes have been recorded on the voting stations prior to the opening of the polls. As the voters cast their ballots on a touch-screen voting station their choices are recorded on the PC memory card. The absentee ballots and provisional ballots are processed through ballot scanners and their votes are recorded on PC memory cards.

After the polls close all of the memory cards from the voting stations in the precincts and from the absentee and provisional ballot scanners are returned to the county elections office for tallying.

Certification of the Voting System: Georgia participates in the Federal Election Commission (FEC) Voting Systems Standards program. This program defines three levels of tests that a voting system must pass before it can be used in Georgia. These three levels are federal tests called Qualification Tests, state tests called Certification Tests, and local tests called Acceptance Tests.

National laboratories selected by and monitored by the National Association of State Election Directors (NASED) Voting System Board administer the **Qualification** tests. During these tests the system is evaluated for accuracy, reliability, availability, and maintainability. In addition, the system is subjected to various environmental conditions that simulate the conditions under which an election system may be transported and stored. A major component of these tests is a line-by-line examination of the source code for the system. This review includes an evaluation of the function of each module of the code to insure that no extraneous code is contained in the system. A complete description of the Qualification tests can be found in the FEC Voting System Standards section on the FEC web site: http://www.fec.gov.

After the system has successfully completed qualification testing it is brought into the State for **Certification** testing. Certification testing is conducted by the Center for Election Systems at Kennesaw State University. Tests are conducted to verify that the voting system complies with the requirements of the Georgia Election Code, the Rules of the Georgia Secretary of State, and the Rules of the Georgia Election Board. A mock election is defined and executed in order to evaluate whether or not the system can be installed and operated by personnel in a typical Georgia election office. During this mock election a sufficient number of ballots is cast to ensure that the system has the capacity to accommodate the maximum number of ballots that may be cast in a Georgia precinct. A major component of the certification tests is to install security features.

The final level of tests, **Acceptance** tests, are conducted in the county offices after the voting system has been delivered and installed. The purpose of these tests are to verify that the system as delivered and installed in the county is complete, is working properly, and is identical to the system that was previously Qualified by the ITA and Certified by the State. The KSU Center for Election Systems also conducts Acceptance tests.

Types of Threats to an Election System: There are two reasons why a person might launch an attack against an election system: to disrupt the election or to commit election fraud. In the first instance, the intent of the perpetrator is simply to disrupt the election, an act of terrorism. Although a terrorist act against an election is disruptive, it is not a threat to the integrity of the election. On September 11, when the twin towers in New York were attacked, there was an election in progress in New York City. One of the precincts was in the shadow of 'ground zero'. The election was completely disrupted. New York election officials re-conducted this election with such quiet professionalism that very few people outside New York are even aware that an election was in progress on that fateful day. No matter how severe, an act of terrorism against an election is disruptive and expensive but it is no threat to the electoral process.

Election fraud is an attempt to alter the outcome of an election. In order to be successful election fraud must go undetected. Once detected election fraud is simply another form of terrorism and can be dealt with accordingly.

The security features installed in the Georgia voting system protect against both terrorism and election fraud, but the main emphasis is on preventing election fraud.

Computer System Security Features: The computer portion of the election system contains features that facilitate overall security of the election system. Primary among these features is a comprehensive set of audit data. For transactions that occur on the system, a record is made of the nature of the transaction, the time of the transaction, and the person that initiated the transaction. This record is written to the audit log. If an incident occurs on the system, this audit log allows an investigator to reconstruct the sequence of events that occurred surrounding the incident.

In addition, passwords are used to limit access to the system to authorized personnel.

Procedural Security Features: There are rigid policies and procedures that control who has access to the election system, when they can access the system, what components they can access, and what function they are allowed to perform. The most familiar of these procedures is the process that a voter must go through in order to cast a vote on the system.

Many of these procedures are directed toward insuring that the correct versions of the system software is initially installed in the GEMS computers and voting stations and, subsequently, testing at various times to insure that this software has not been altered.

To insure that the initial installation of the software is correct, the following steps are rigidly enforced.

- The State does not accept software from any source except the ITA that conducted the NASED Qualification Tests on the software. When the ITA completes Qualification Testing of the software they submit to the KSU Election Center a copy of the source code and the resulting object code.
- As a part of the State Certification Testing the KSU Election Center prepares a validation program, similar to a virus detector program, that is subsequently used to verify that versions of the software installed in the county systems is identical to the software that the KSU Center certified. This validation program is structured such that it provides a 1/1,000,000,000 chance that someone could alter the software without being detected.
- When the software is installed in a county system, a member of the KSU Center travels to that county and runs the validation program to verify that the installed software is correct.
- This validation program is routinely run before an election is begun to verify that the software is correct. It is run again after the election to verify that the software did not change during the election.
- The validation program can be run at any time that an incident occurs that might potentially alter the software. An example of such an event might be a nearby lightning strike that caused the GEMS computer to crash.

Physical Security Features: The first line of defense in any system is physical security. The following is an overview of the physical security implemented in State elections.

- The GEMS computers are kept in locked offices within the county election offices.
- The GEMS computers are not connected to any communication system, including the Internet, and contain no software other than the Windows operating system and the Global Election Management System object code.
- A security program, similar to a virus detector program, is run against the Windows operation system and the GEMS object code prior to beginning the definition of an election to verify that the code has not been altered. This program is repeated after the close of the election to verify that the code did not change during the election.
- No person is allowed access to the GEMS computer until his or her identity has been clearly established by the county Election Superintendent.
- The voting stations are stored in their voting booth cases in stacks of five in a locked county warehouse facility.
- The PC memory cards in the touch screen voting stations are in a locked compartment. The Precinct Manager is the only person in a precinct with a key to this compartment.
- After the polls close a summary report of the votes cast in the precinct is posted on the precinct door.

- The PC memory cards from a precinct are transported from the precinct to the county elections office by a sworn election official or a sworn law enforcement officer.
- The area of the precinct that contains the voting stations is secure. A voter is not allowed to enter this area until a voting station is available for his or her use.

Specific Comments: In the following paragraphs we address specific comments that have appeared in the press and open literature.

"If the only way you know that it's working incorrectly is when there's four votes instead of 1,200 votes, then how do you know that if it's 1,100 votes instead of 1,200 votes? You do not know.", Rebecca Mecuri, Professor, Bryn Mawr College, Washington Post, New Voting Systems Assailed, March 28, 2003

In a Georgia precinct there are three separate manual counts of the number of voters that cast ballots in the precinct. These are 1) the number of people that fill out a registration slip (called a voter's certificate), 2) the number of people checked on the voter registration list, and 3) the numbered list of voters (i.e. the number of ballots issued). When the polls are closed these three numbers are audited against the number of ballots recorded as cast on the voting system. Any discrepancy between these four totals is immediately obvious and must be accounted for in order to close the precinct.

"No official at Diebold or the Georgia Secretary of State's office has provided any explanation at all about program files contained in a folder called 'rob-georgia' on Diebold's unprotected FTP site. Inside 'rob-georgia' were folders with instructions to 'Replace what is in the GEMS folder with these' and 'Run this program to the C-Program Files in Winnt System32 Directory' ". Beverly Harris, Black Box Voting: Ballot-Tampering in the 21st Century, http://www.blackboxvoting.com, March 3, 2003

Apparently, there was an FTP site that Diebold employees used to store and transfer versions of the system that were under development. The contents, of even existence, of the 'rob georgia' folder has not been established.

However, for the sake of this discussion, we will assume that the FTP site existed, that the version of the GEMS system used in Georgia was on that FTP site, that the 'rob georgia' folder existed, and that there was a rogue employee at Diebold that intended to use the 'rob georgia' folder to corrupt the Georgia voting system.

This would have had absolutely no effect on the election system as implemented in Georgia. The State does not obtain its election system code from an FTP site or even from Diebold. The process is as follows:

- The vendor, Diebold, submits the source code to the ITA.

- The ITA conducts a line-by-line examination of the source code to determine that no extraneous code is present (i.e. that all code presented has a direct relationship to the functions of conducting an election).
- After completing their evaluations, the ITA oversees the compilation of the source code into object code.
- The ITA, not the vendor and certainly not an open FTP site, provides the KSU Election Center with the source code, the object code, and various related files.
- The KSU Election Center conducts Certification Tests on the code provided by the ITA.
- After successful completion of Certification Tests the vendor is allowed to install the certified object code in the county computers.
- The KSU Center conducts audits to verify that the code that the vendor installs in the counties is identical to the code that was obtained from the ITA.

"A patch to the underlying operation system - Windows - can slip through without scrutiny." Beverly Harris, Black Box Voting: Ballot-Tampering in the 21st Century, http://www.blackboxvoting.com, March 3, 2003.

This comment assumes that the State of Georgia allows changes and/or upgrades to the Microsoft operating system. This is not the case.

The vendor, Diebold, submits to the ITA a specific version of the operating system and a specific version of the election software. This specific version of the operating system and the election software undergoes ITA testing and State Certification testing. The State Certification is for this *specific* version of the Microsoft operating system and the Diebold election system. After State Certification any change to either the Microsoft operating system or the Diebold election system voids the State Certification.

If a change to either the Microsoft operating system or the Diebold election system becomes desirable or necessary, this change voids the State Certification. The revised system then must then go back through the entire ITA Qualification and State Certification process.

"It requires one programmer at the company who has a political agenda or who has been bribed or somebody who can break into the company's network, who can hack the code when they're not looking," David Dill, Professor, Stanford University, High Tech Train Wreck, Creative Loafing, April 2, 2003.

This is the vendor version of the comment above and is equally unlikely. Let's look at what must transpire in order for a rogue employee of the vendor to effectively commit election fraud.

First, (s)he must figure out how to defraud an election that has not yet been defined and that will occur several years in the future. Since the races, much less the candidates, have not yet been defined the best you can hope for is to favor certain parties. In Georgia this

is not a trivial matter. The State does not use the party affiliations built into the election system. Instead, the State embeds the party affiliation in the candidate name field. Thus, the rogue code must parse the name field looking or "R" or "Rep" or "REP" or "Republican" or "REPUBLICAN", and “D” or “Dem” or “DEM” or “Democrat” or “DEMOCRAT”, etc.

Second, in a primary election all choices on a given ballot belong to the same party, it would be impossible to favor an, as yet, undetermined candidate in a primary election.

Finally, for this approach to election fraud to succeed, this code must lie dormant during all testing phases, ignore a primary election but become active during a general election, and lie dormant during all post election testing.

The code required to accomplish the foregoing is substantial. It is extremely unlikely that this amount of code would escape detection by the ITA during Qualification Testing.

Finally, if all else fails and rogue code finds its way into the State election system, it would be detected during State certification tests. The contention is that this code could be cleverly devised to become active only on the dates of a general election. When we conduct our mock election we set the date on the computer to the date of a general election.

"A person could insert a memory card into a voting machine that would change the program on the machine.", Anonymous.

This conjecture assumes that one can simply walk up to a voting station in the State and insert a PC memory card. It is not this simple.

The following steps would be necessary in order to commit election fraud by altering the code in the voting stations employed in Georgia.

First, one would have to obtain the code installed in the voting station and alter it to suit their purpose. This is no small feat but, for the sake of this discussion, let us assume that it is done. Assume that the perpetrator has in their possession a supply of PC memory cards that can alter the code in a voting station in such a way as to alter the outcome of an election. One must now get this bogus system installed in the voting stations.

The voting stations can be attacked either before or after they are installed in the precincts. Before they are installed in the precincts the voting stations are stored in county warehouse facilities. In these warehouses, the voting stations are enclosed in their voting station cases and stacked five high. To alter the voting stations in this environment, one would have to gain access to the warehouse, remove the voting stations from the stacks, open the cases, unlock the memory card access door (having obtained a key from somewhere), insert the bogus PC memory card, boot the voting station to install the bogus code, shut down the voting station, remove the bogus PC memory card, close

the case, and return the voting station to the stack. All of this must be accomplished without being detected by any of the county warehouse employees.

To attack the voting stations in a precinct one would have to gain access to the secure area of the precinct. The only people allowed in this area are poll workers and registered voters. Poll workers only work in one precinct and do not move from precinct to precinct. Altering the voting stations in only one precinct is not likely to alter the outcome an election. Thus our perpetrator must either be or impersonate a registered voter in the precinct. Once in the secure area, the perpetrator must remove the right-hand security screen, unlock the memory card access door (having obtained the key from somewhere), remove the PC memory card in the voting station and insert the bogus PC memory card, reboot the voting station, remove the bogus PC card and re-insert the original card, reboot the voting station, lock the access door, and replace the security screen. All of this must be accomplished without attracting the attention of any of the poll workers, candidate poll watchers, or party poll watchers. This procedure must then be repeated for the other voting stations in the precinct.

The above scenarios describe the effort required to alter a single voting station. In order to impact a statewide race our perpetrator must modify a significant portion of the 22,000 voting machines in the State. To impact an election in Fulton or DeKalb County one would have to alter a significant portion of 3,000 voting stations. On the other hand, if one's ambition were to be a county commissioner in Talliaferro County, population 2077, he would only have to alter 8 voting stations.

"When Georgia debuted 22,000 Diebold touch screens last fall, some people touched one candidate's name on the screen and saw another candidate's name appear as their choice. Voters who were paying attention had a chance to correct the error before finalizing their vote, but those who weren't did not.", Dan Keating, Washington Post Staff Writer, New Voting Systems Assailed Computer Experts Cite Fraud Potential, Washington Post, March 28, 2003.

"In Georgia, newly using touch-screens, some voters reported their votes being recorded for other candidates", Peter G. Neumann, SRI, The 2002 General Election, The Risks Digest, Volume 22, Issue 36, November 6, 2002.

During the 2002 General Election in Georgia there were five reported instances of persons touching a name on the ballot and adjacent name lighting up. In each case, technicians were sent to the precinct, but in each case the problem could not be duplicated.

This can occur as a result of a calibration error on a voting station. If the voting station is not perfectly calibrated there will be a small area between two names where pressing in this area will register for the wrong name. Since most voters vote with the end of their finger, not with a sharp instrument such as a stylus, the voting station would have to be significantly out of calibration for this error to occur.

When it does occur it is immediately obvious and easy to correct. The voter simply de-selects the wrong name and selects the right name. If the voter is not paying attention and misses this error when it occurs, (s)he gets another chance to correct the error when (s)he reviews the summary screen at the end of the ballot.

If the situation persists, the voter is moved to another voting station to continue voting and the poll manager recalibrates the errant voting machine. It takes approximately two minutes to re-calibrate a voting machine.

"Computerized voting equipment is inherently subject to programming error, equipment malfunction, and malicious tampering. It is therefore crucial that voting equipment provide a voter-verifiable audit trail, by which we mean a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, and is difficult or impossible to alter after it has been checked. . . . The paper ballots must be submitted by the voters, to be available for counting or recounting and to avoid vote-selling. The votes on the paper ballots must be regarded as the definitive legal votes, taking precedence over electronic records or counts. ", David Dill, Professor, Stanford University, http://verify.stanford.edu/evote.html, January 20, 2003.

Complex problems rarely have simple solutions. If all of the problems with an electronic voting system could be solved by the seemingly simple act of adding a printer to each voting station and printing paper receipts election officials would be clamoring for this to happen. They are not. Here are some of the reasons.

There are logistical problems associated with the introduction of paper ballots.

- The presence of the paper supply in the voting station would increase the weight of the voting station. When fully loaded with paper, as at the opening of the polls, the current voting stations that provide paper receipts weight in excess of forty pounds, more than a typical poll worker is capable of lifting.
- The component of an electronic system that is most likely to malfunction is an electro-mechanical component. Printers are more mechanical than electrical. Thus, the introduction of the printer to a voting station greatly increases the probability of the voting station failing during an election.
- Poll workers must be trained to replace paper and ink.
- Technicians must be available to replace failed printers.
- Finally, there is the expense associated with the purchase, installation, and maintenance of a large number of printers (22,000, and counting, in Georgia).

The contention is that the voter will check the paper receipt for accuracy before his ballot is cast. Georgia law requires that voters be allowed to change their ballots up to the time that the ballot is cast. Therefore, a voter who does not like what is on the paper ballot must be given an opportunity to change it, as many times as he wishes. The present procedure for spoiling a paper ballot includes a requirement that the spoiled ballot be placed in an envelope to be available for auditing the number of ballots issued versus the number of ballots cast. If the voter can change his mind at random and print as many

paper ballots as he wishes, how is the poll worker to know how many ballots have been spoiled and ensure that the correct paper ballot is deposited in the ballot box?

How do you handle the situation where a voter casts his electronic ballot before he notices that the paper ballot, for whatever reason, cannot be read? Now we have a valid electronic ballot, but no corresponding paper ballot. If we now use the paper ballots in any official capacity we have disenfranchised this voter.

A similar situation exists when a voter casts his electronic ballot and then insists that his paper ballot is incorrect. How do we determine whether this is the result of a voter error or a system error? If the voter admits to committing an error there is no way the error can be corrected. We cannot let him obtain a paper ballot by voting again on the electronic system and changing the paper ballot introduces a discrepancy between the electronic ballots and the paper ballots.

It finally gets down to a question of need. The primary argument in favor of a paper receipt is that it could be used to check the accuracy of the electronic system. The fallacy in this argument is that the paper receipts would, in fact, be less accurate than the electronic ballots they are supposedly checking. The current DRE voting systems have been tested to an accuracy of better than one part in ten million, as per the FEC Voting Systems Standards. Thus, the paper receipt is not needed to insure accuracy. In fact, our past experience with manual counts of paper ballots proves that they cannot consistently achieve that level of accuracy.

The paper ballots could be printed in a format that is machine-readable and counted on another computer. But that would put us in the rather peculiar position of saying that we do not trust the computer that printed the ballots but we trust the computer that counted them.

Summary: In conclusion, we recognize that there is no such thing as a 100 % secure computer system. Yet we are willing to fly on airplanes that are controlled by computers. We allow a heart-lung machine controlled by a computer to monitor and control the vital functions of our body during an operation. In many phases of our lives we are willing to submit to various computer controlled situations. Why should we not extend the same level of confidence to our voting systems.

We do not pretend that the security features described above make the State's voting system completely safe from attack. We do believe, however, that these features reduce the chance of a successful election fraud in the State of Georgia to better than one in one billion.

About the Author: Brit Williams is a Professor Emeritus of Computer Science and Information Systems at Kennesaw State University. He was a consultant to the FEC during the development of the FEC Voting System Standards in 1990 and again in 2002.

He is currently a member of the NASED Voting Systems Board and Chair of the NASED Voting Systems Board Technical Committee. He has been conducting certification evaluations of computer-based voting systems for the State of Georgia since 1986. He also assists the states of Pennsylvania, Maryland and Virginia with certification evaluations of computer-based voting systems.