Jerry J. Lobdill
DFA Tarrant County, TX
8/20/2006 10:10 AM

Designing
Mandatory Election Audits

By
Jerry J. Lobdill

This paper is about designing mandatory election audits. All designs for such audits use statistical sampling to achieve a high probability of detecting tampering in an election. The trick in doing this is to avoid errors in modeling the processes that are operative, assuming randomness inappropriately, for example, or applying the central limit theorem inappropriately to simplify computations.

One recently proposed method for designing mandatory election audits assumes that all polling stations are equally likely targets for attack[1]. All polling stations are grouped together to make up a population from which a random sample of stations is selected for audit. The Poisson hypergeometric formula (See Equation (6), below) is used to determine how many polling stations should be audited to achieve a 0.95 probability of detecting tampering.

Such a method ignores information available at the time the audit is to be designed that would allow cluster sampling to achieve the same probability of detecting tampering with fewer polling stations in the audit. Indeed, as will be shown, by performing the audit on the cluster having the highest probability of being corrupt, tampering may be detected with very few polling station audits.

How Elections Are Conducted

We consider only elections that are conducted under the supervision of a state's Secretary of State. Such elections involve races for county, state, and federal offices. Such elections are administered by county election authorities and are conducted precinct by precinct. Sometimes precincts are combined at one polling place. Each precinct or polling place is administered by Party officials. At the close of polls on election day the officials at each polling place carry out prescribed procedures for tallying votes at the polling place and preparing a report. All reports are taken to a central election headquarters where the tallies are combined into a countywide tally. The incremental tally is announced periodically during the evening as results come in and are combined. At the conclusion of this process the election results are certified by the election officials. Candidates may call for a recount if their race results were close enough to permit a recount. (In Texas only races closer than 10% are eligible for recount.) It would be in a period before results are certified that a mandatory audit would be conducted.

Mandatory election audits

One of the conclusions of the June 28, 2006 landmark study, The Machinery of Democracy: Protecting Elections in an Electronic World, by Brennan Center Task Force on Voting System Security, Lawrence Norden, Chair, June 2006 was that voter-verified paper audit trails and/or paper ballots read and tallied by a Precinct Count Optical Scan (PCOS) machine were of little value without a mandatory election audit.[2] This study was concerned with defining and evaluating threats to electronic voting, not with design of audits. The Brennan report provides an in-depth analysis of the threat and identifies over 120 different attacks that could be launched against elections. Although the focus of the study was attacks on electronic systems of various types, the attacks catalogued all are precinct or central tally center based. In that regard they encompass many, if not all, of the ways in which any PCOS election system can be attacked.

Attacks on an election may occur at the precinct level or at one or more of the subsequent combination tally centers. The kinds of attacks differ depending on the situation. The report focused on a particular fictional example for a state named "Pennasota". The data were a combination of results from the 2004 election, and the race targeted for audit was the governor's race, which had a vote margin of 2.32%.

[1] ElectionArchive.org document: "How Can Independent Paper Audits Detect and Correct Vote Miscounts?"
[2] Recommendation #1, Brennan Report, p 87

Since mandatory audits would be defined and prescribed by state law this paper necessarily assumes the existence of such a law. The presumed law prescribes that each county will be responsible for conducting a mandatory audit of each election that is overseen by the county elections authority. The audit will be designed to detect tampering in the countywide race that has the smallest margin of victory at a probability of detecting tampering of 0.95 in that race. Audits will be conducted on a polling place basis, and in primary elections there will be an audit on the Republican primary and the Democratic primary elections. If the audit shows election irregularity then a full hand recount of all ballots cast in the county is mandated.

In this paper we consider an audit design methodology that places the responsibility for audits with the county election authority, the lowest level authority in the overall election system. In order to design an audit methodology for a county it is useful to look to the threats identified in the Brennan Report because they are universal and apply to the attacker, who will attack (change votes) at the precinct level. Quoting from the Brennan Report, p 22:

> "We have assumed that our attacker would prefer that her actions not raise undue suspicion. Accordingly, we have placed some limits on the type of actions our attacker could take. …these limits can further help us determine how difficult a particular attack would be (i.e., how many informed participants the attacker would need to involve.)
>
> "Perhaps most importantly, we have assumed our attacker would not want to add or subtract more than 10% of the votes for a candidate in any one county or switch more than 5% from one candidate to another), for fear that a greater change would attract suspicion.
>
> …we have put limits on the number of votes an attacker would seek to change in a single polling place or a single machine. We have assumed that a swing of greater than 15% in any single polling place or 30% on any single machine would attract too much suspicion."

In this paper the example election data shows that the race with the smallest vote margin is a race at the county level and not the state or federal levels.[3] The election is the 2006 primary election and the audit we are concerned with is that of the "Republicrat" Party primary. We assume that all voting machinery produces voter-verified paper ballots that are deposited in secure containers.

The postulated attack would be a "wholesale" attack[4] designed to switch sufficient votes to change the outcome in the race that had the minimum vote margin in the county. The attacker would be generally guided by the principles stated in the quotation above. If we accepted all of these principles, however, this would result in a rule that unless one race had a margin not greater than 10% of the vote in the county, there would be no mandatory audit in that county. While present Texas law prohibits a recount if the vote margin in a race is 10% or more, we wonder why an attacker, knowing this, would not make the margin somewhat higher than 10% if it would result in no recount. Therefore, we suggest that an audit should be done even if there is no race closer than 10%. In our example, the margin is 11.79%, and we conduct an audit under a proposed state law that would not limit mandatory audits according to this criterion.

Modifying Brennan Report Assumptions

The example election data presented in the Brennan report is only detailed enough to permit study of methods of attack on the electronic voting system and how they might be countered. The design of mandatory audits requires a much finer grained analysis of election data.

The attacker's rules of engagement are to attack as few polling places as possible to switch the expected (forecast) required number of votes, and to switch no more than 7.5% of the votes at any precinct.

[3] Note, however that if a state level or national level candidate happened to have the smallest margin of votes that race would be used to design the county audit.

[4] Brennan Report terminology- indicates that all voting machines have the same Trojan Horse software installed prior to the election.

The attack we presume is similar to that identified in Brennan as PCOS[5] Attack 41 (p 78-81). It is the easiest and therefore most probable attack. It is accomplished by inserting Trojan Horse software into each PCOS unit in the county. This software is awakened if the vote count exceeds some preset minimum number of votes (selectable in our case). This protects the attack from discovery during parallel testing[6] and also eliminates the corruption of PCOS machines with low final vote counts. The Trojan Horse software is inserted at the time the PCOS machines receive their election-specific code; i.e., before the election. Because the attacker does not know in advance how the votes will be distributed among the polling places, or what the final margin will be, the preselected minimum number of votes required to trigger the attack and actual polling place traffic will dictate the number of polling places that actually fall under attack.

In this scenario the attacker cannot design her attack with knowledge of the actual margin and does not know how many PCOS machines (polling places) will be attacked. She would err on the side of greater probability of turning the election in her favor if she believed there was sufficient risk of losing. She would probably rely on advance polling to make this decision

Since we design our audit after the central tally has been concluded and detailed vote data are available, we base it on our perfect knowledge of, among other things[7], the actual margin, M, the actual vote counts registered at the polling places, and we design for the minimum possible number of PCOS attacks, B, necessary to turn the election.[8] We also assume that PCOSs with vote counts smaller than some conservative guess at the attacker's choice of Trojan Horse trigger need not be included in the total population, N, of polling places considered in the Poisson formula[9]. Finally, we design for a 0.95 probability of detecting the attacker.

Concluding Remarks about Mandatory Audits

We design the audit based on a presumed attack doctrine that, in itself, involves guesses that determine the outcome of the attack. Our design involves guesses at what the attacker's choices would be. Therefore, when we set up the Poisson formula we have made assumptions about two of the parameters that determine the probability calculated. These two parameters are (1) total number, N, in the population of possibly corrupted polling places, and (2) the number of corrupted polling places, B. Unfortunately, there is no way to avoid this uncertainty.[10] We obviate this problem by designing the audit based on the race with the smallest margin. All other races will have a higher probability of irregularity detection than the race we design for.

[5] PCOS means Precinct Count Optical Scan
[6] Brennan Report, p 18-19, 53-61, 88-89, 95
[7] We also know the total number of registered voters in each precinct, the percent of early votes at each precinct, the number of undervotes at each precinct, the actual vote count and margin precinct-by-precinct even if multiple precincts vote at polling places. This information is available at the time we must design the audit.
[8] The latter assumption assures that our audit will detect the attack with at least 0.95 probability, since the attack will necessarily involve no fewer than the number of PCOS units we assume.
[9] The inclusion of all polling places would result in oversampling for the audit.
[10] As a professor of mine once said, "When you deal with probability, you'd better be willing to take a chance."

Jerry J. Lobdill
DFA Tarrant County, TX
8/20/2006 10:10 AM

Mandatory Election Audit Design—
Lonesome Dove County, Texas, Republicrat Primary Election, March, 2006

Probability Formulas Used

Consider a set of n independent events, A_1, A_2, A_3, … A_n whose probabilities of occurrence are $P(A_1)$, $P(A_1)$, $P(A_2)$, … $P(A_n)$.

The probability of A_1 or A_2 or both occurring is given by $P(A_1) + P(A_2)$. (1)

The probability of A_1 and A_2 both occurring is given by $P(A_1)xP(A_2)$.. (2)

The probability that A_1 does not occur is given by 1- $P(A_1)$. (3)

The number of combinations of N things taken r at a time is given by

$$\binom{N}{r} \equiv \frac{N!}{r!(N-r)!}$$, where $N!$ is N factorial or Nx(N-1)x(N-2)...3 x 2 (4)

Poisson's Hypergeometric Formula

The famous mathematician Siméon-Denis Poisson (1781-1840) published the hypergeometric formula that is central to the election audit problem in an 1837 monograph. He had used this formula in connection with elections in France. Today we are faced with designing election audits in the United States, and we naturally turn to Poisson's work for the necessary math.

Given a total of N marbles that have one of two characteristics (say white or black marbles), if there are B black marbles and N-B white marbles, then if a random sample of S marbles is drawn from the total, the probability, P, that there are exactly b black marbles in the sample is given by Poisson's Hypergeometric Formula:

$$P(b,S,B,N) = \frac{\binom{B}{b}\binom{N-B}{S}}{\binom{N}{S}} \quad (5)$$

The probability that there are exactly zero black marbles in the sample of S marbles is computed by setting b = 0. Then the probability that there is at least one black marble in the sample, S is given by:

$$1 - P(0,S,B,N) = 1 - \frac{\binom{B}{0}\binom{N-B}{S}}{\binom{N}{S}} \quad (6)$$

This formula is used in mandatory audit design to determine the sample size, S, required to assure a 0.95 probability that the sample contains at least 1 corrupt polling place when there are B corrupt polling places in the population, N.

Designing the Election Audit

The data for this example is based on the Tarrant County, TX (which we will call Lonesome Dove County since we are modifying some of the results) March 2006 primary election. The smallest margin in this election is assumed to be that for the Republicrat Party County Chair race. The election margin was 1608 votes in favor of the incumbent.

Certain data from the election has been altered for purposes of this example. The actual election was concluded without an audit or a recount. Because the margin of votes was greater than 10% for the closest race, the challenger did not have an option under Texas law to ask for a recount.

We cluster early votes by polling place and we cluster Election Day votes by polling place in selecting samples for audit. We do this because in Texas early voting fraud is rampant and early votes are more likely to be corrupted than Election Day votes.

The following data describe the election data for this example.

Lonesome Dove County Election Data, March 2006

Countywide Total Registered Voters	888517
Total votes cast in closest Republicrat primary race	14553 (includes overvotes and undervotes)
Incumbent votes	1100 Mail, 1470 Early, 5053 Election Day, 7623 Total
Challenger votes	283 Mail, 1588 Early, 4144 Election Day, 6015 Total
Overvotes	12
Undervotes	903
Number of Polling Places	211
Number of Precincts in Lonesome Dove County	634
Number of PCOS units per Polling Place	2 (One for Demicans and one for Republicrats)

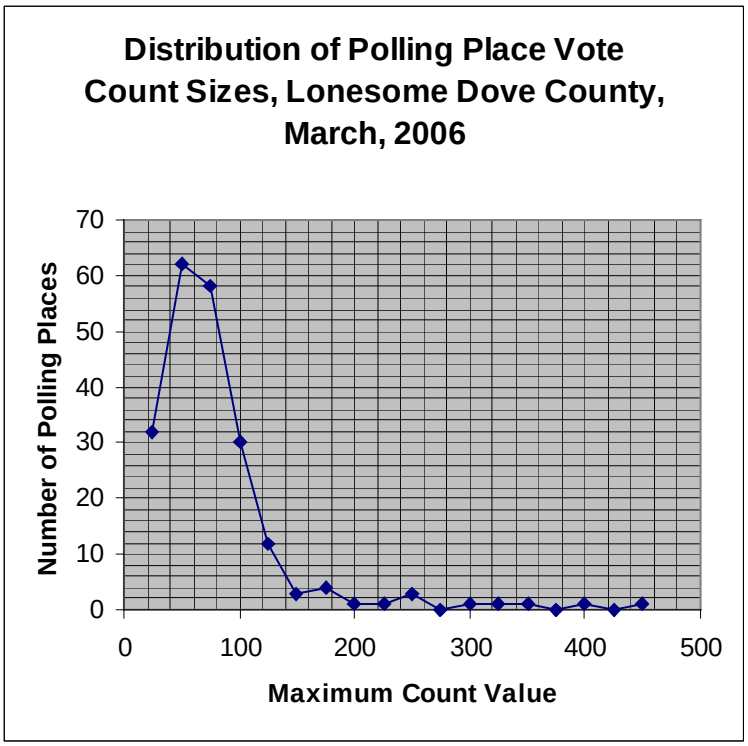

FIGURE 1

Histogram
50 count bins

The tight clustering of data and the long right hand tail suggests analysis of the tail. The data suggests that perhaps the Trojan Horse trigger was around 190-200 votes if there was an attack.

FIGURE 1 Frequency Distribution of polling place vote counts

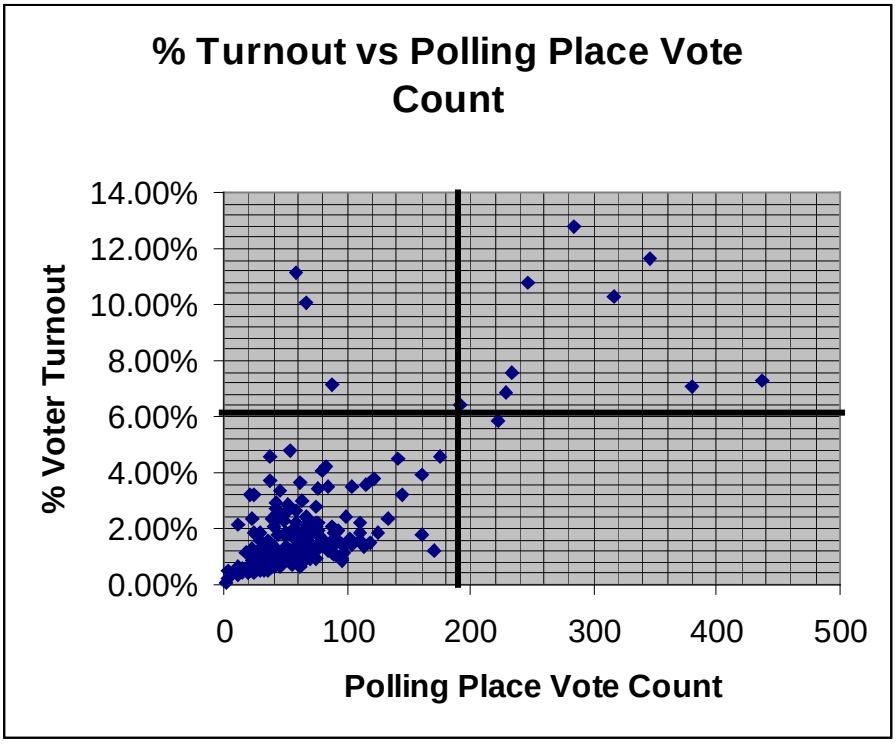

FIGURE 2

Mean = 1.97%
Sigma =2.06%

6.1% = Mean + 2 Sigma
Assumed Trigger for Trojan Horse = 190 votes

The voting stations in the upper right sector serve areas that are known for vote fraud.

FIGURE 2 % Turnout of registered voters at Republicrat polling places (% of total registered voters)

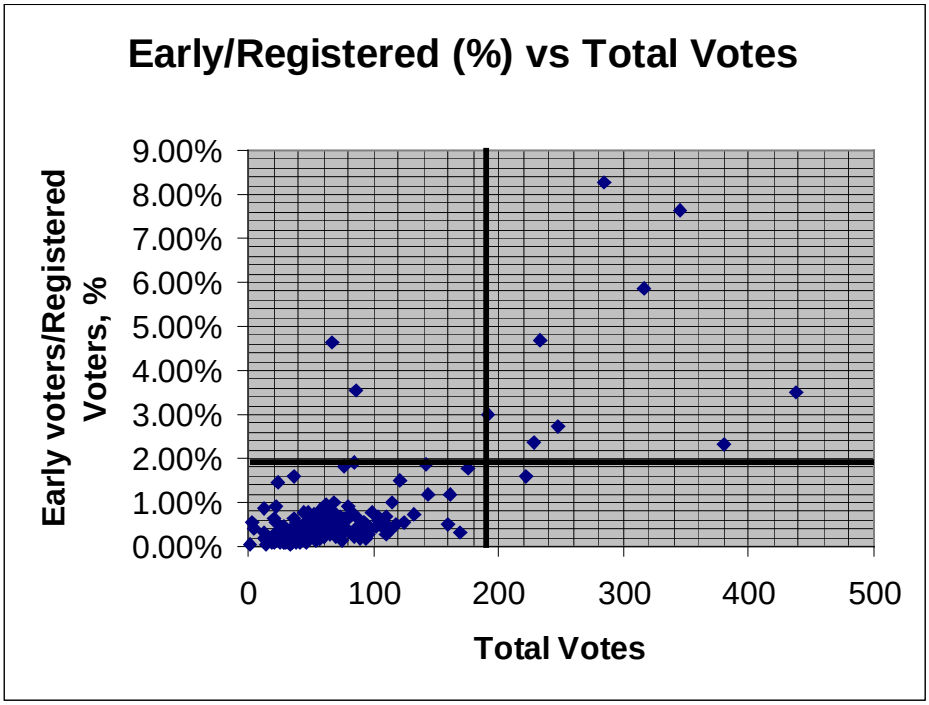

FIGURE 3

Mean = 0.65%

Sigma = 0.64%

Mean + 2 Sigma = 1.93%

The upper right sector contains the same polling places as the upper right sector of FIGURE 2. Hmmm…

FIGURE 3 % Turnout of early voters at Republicrat polls

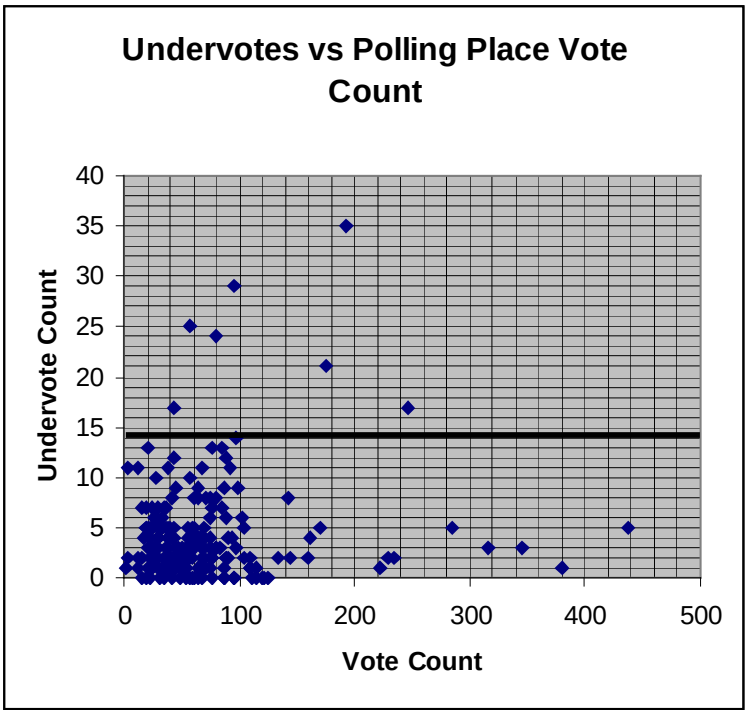

FIGURE 4

Average Undervote 4.28 votes
St. Dev 4.87 votes

Avg + 2* St Dev = 14.02

FIGURE 4 – Undervote Count vs Vote Count

Analysis of the polling stations that exceeded an undervote count of 2 sigma above average revealed that all of them were also high percent turnout and high early voting stations. This could indicate tampering at these polling stations. FIGURE 4 added evidence that suggested clustering these stations.

ATTACKER SELECTIONS

Trojan Horse Trigger	190 votes
% votes to switch at each polling place (% of total)	7.5%

RESULTS OF ATTACK

Number of polling places attacked	9
Number of votes switched	206
Margin change in favor of Incumbent on Election Day	412
Early Votes added to Incumbent through fraud	800

AUDIT DESIGN

Number of polling Stations with more than 2 sigma above mean deviation	9[11]
Number of assumed corrupt polling stations in this cluster @ 1/3	3
Number of polling stations to randomly select from this cluster to audit	5
Number of polling stations below 2 sigma threshold	202
Number of assumed corrupt polling stations in this cluster @ 10%	20
Number of polling stations to randomly select from this cluster to audit	27[12]
Number of Mail ballots cast	1383
Number of assumed corrupted mail ballots	1000[13]
Number of Mail ballots to audit	3[14]
Total number of polling places audited	32

CONCLUSIONS

This audit would detect the attacker's tampering and would trigger a complete recount. The sequence for the audit should be to first audit the 5 polling stations selected from the first cluster of 9, which had an abnormally high % turnout, a high rate of undervotes, and a high vote count from the same 9 polling stations. If corruption is detected, the audit is over, and a full countywide recount is done

If this audit had been designed without clustering we would have lumped all 211 polling places together and assumed 2% or 5% corruption, and using Equation (6) we would have calculated sample sizes of 110 or 49 respectively instead of a maximum of 32 with the possibility of a much smaller number. This demonstrates the value of clustering the data to improve fraud detection capability and decrease the number of polling stations to be audited.

[11] We do not know what vote count trigger level the attacker has set, so we determine this by looking at high count stations that also have more than a 2 sigma increment in % Turnout (FIGURES 2, 3)
[12] Use Equation (6) with P = 0.95, N = 202, B = 20, find S = 27
[13] Mail ballots are bought for $2 per vote. This is a good return on investment if one is a cheater.
[14] Use Equation (6) with P = 0.95, N = 1383, B = 1000, find S = 4