Olde Fashioned Legal Loopholes Allow Rigging of Hi-Tech Elections

(January 30, 2007) - Contributed by Howard Stanislevic and John Washburn

The following is a brief discussion of how election integrity can be compromised by taking advantage of loopholes in election reform legislation. The authors believe that any such legislation should be judged by its ability and intent to mitigate the risks discussed herein.   We will focus on four major loopholes: Loophole #1 Internet connections NOT banned for Election Management Servers Loophole #2 High failure rates are allowed for equipment; equipment allowed to remain in service Loophole #3 No statistically meaningful audits Loophole #4 No or inadequate instructions to direct voters to verify voter verifiable records   Each of the above loopholes provides a different set of possible effects which individually or together can alter the outcome of an election.

Loophole #1:

Although Internet connections may be banned for voting machines on which votes are cast, Election Management Servers (EMS) such as Diebold's GEMS, ES&S' Unity and Sequoia's WinEDS are allowed to be connected to the Internet.

Possible Effects of This Loophole:

1.1. Ballot definition programming is corrupted, or a "Trojan Horse" (per the Brennan Center's "Machinery of Democracy" report) is introduced on this server in one of two ways at any time PRIOR to the election:

1.1.1. An outsider gains access to the EMS server via the Internet and loads the malicious code, or just logs in and makes changes to the election-specific ballot definition files that would cause vote switching to occur. We know this capability exists because it's been documented by VotersUnite. See: "Vote Switching Provided by Vendors" and in numerous accounts in the press after every recent election. Pottawattamie County, Iowa is one such high profile example. It's a simple one, probably accidental, but much more complex and subtle attacks are possible. See: "CNN's Lou Dobbs Investigates Programming Errors in Iowa".

1.1.2. An insider intent on rigging an election, who might normally be watched or checked by someone of a different political party where the EMS server is physically located, can work unobserved from home via the Internet. By "telecommuting", she logs in to the EMS Server with her Blackberry, laptop or other Internet-connected computer from home (or an undisclosed location) and proceeds to rig the election using the technique(s) described above in 1.1.

1.2. The corrupt election configuration (ballot definition file), or Trojan Horse, is loaded into every DRE and Scanner in the jurisdiction from the EMS server per the usual procedures, spreading the bad election definitions or Trojan Horse to every machine or optical scanner on which votes are going to be cast, or perhaps a targeted subset of machines or scanners. No Internet connection is required to do this. It can be done using memory cards, a local-area network, dial-up or a private modem network. This goes undetected because, as Dr. Ed Felten and his team at Princeton have shown, it's possible to design viruses to evade detection by Logic and Accuracy tests.

1.3. The ballot definition file that is disclosed to the public (assuming there is a requirement for such disclosure), which is also the one used to perform the L&A test, is the correct ballot definition file (i.e., NOT corrupted). So even an audit of this programming would not show any problems. However, this is NOT the file or Trojan Horse that is loaded in some or all the voting machines or scanners in the jurisdiction to actually run the election; that was introduced to the EMS server via the Internet.

1.4. In addition to vote switching, installing the Trojan Horse or corrupt ballot definition code originally introduced to the EMS server via the Internet can cause various forms of Denial of Service attacks aimed at DRE voting systems which must be up and running in order for voters to cast their votes. For example, as a selective Denial of Service attack, DREs could be programmed to generate undervotes only when votes were cast for a specific candidate. Or DREs could be programmed to crash altogether, disenfranchising voters in certain partisan strongholds to weaken support for all the candidates of a particular party as a more general Denial of Service attack. This latter risk does not exist with optical scanners since hand-marked paper ballots allow fail-safe recording of voter intent.

1.5. After the election, the precinct totals are checked and transparently aggregated and they all match the "central tabulator" totals on the EMS server 100%. But the election has already been rigged by switching or deleting votes on some or all machines or scanners in the jurisdiction AS THEY WERE CAST, using the malicious ballot definition file or Trojan Horse previously loaded onto the EMS server via the Internet -- perhaps months before the election -- as a consequence of Loophole #1 which allowed the EMS server to be connected to the Internet in the first place.

1.6 Voters are disenfranchised.

1.7 The wrong candidate is elected.

Loophole #2:

Allow a high failure rate for all voting systems, provide emergency paper ballots, but do NOT require failed machines to be taken out of service.

Federal standards allow nearly 10% of all DREs in the nation to fail in a 15-hour election day. Therefore the above Denial of Service attacks will be indistinguishable from "normal" in situ failures allowed under the national standards. See "DRE Reliability: Failure by Design?"
A law guaranteeing a voter a paper ballot without requiring faulty machines to be taken off line allows subsequent voters to be denied service.

Possible Effects of This Loophole:

2.1 Voters are disenfranchised.

2.2 The wrong candidate is elected.

Loophole #3:

Require voter verifiable paper records, trails or "ballots" to be produced by the voting system but do NOT require manual audits of sufficient size or quality to detect vote count discrepancies that can change the outcomes of elections.

Much has already been written about this subject, so there is no need to belabor it here. It can be considered to be a loophole however since audits are really the only thing in the law standing between detection or certification of incorrect electoral outcomes. See "Random Auditing
of E-Voting Systems: How Much is Enough?", "Larger Audits Required to Confirm 2006 US House Races", and "On Estimating the Size of a Statistical Audit". Suffice it to say that any audit not based on a probability of outcome-altering miscount detection is an audit in name only.

Possible Effects of This Loophole:

3.1 The wrong candidate is elected.

Loophole #4:

The law requires voter verifiable paper records (VVPARs) but does NOT require voters to be properly instructed to verify their votes on the paper records because:

- Voters may not speak the language in which such instructions are written;

- They may have a disability that prevents from seeing such instructions
posted at a polling place;

- There are not enough signs displaying said instructions at the
time or the place when and where the votes are actually cast -- i.e., on
the voting machines or in the voting "booths."

Possible Effects of This Loophole:

4.1 If discrepancies between the DRE Summary screens and the VVPARs are NOT detected by the voters, even a full recount of VVPARs would NOT detect such discrepancies (because the VVPARs can be programmed to match the electronic vote tally). Note that this particular risk does not exist with optical scan systems.

4.2 The wrong candidate is elected.

Since the connection of the EMS server to the Internet allowed in Loophole #1 above poses an existential threat to elections (via denial of service attacks) and can also allow changes to the outcomes of elections to be made in advance (via undetected vote switching due to Trojan Horses and/or corrupt ballot definition programming), it's clear that any election integrity legislation worthy of the name should prohibit connections of EMS servers to the Internet, especially connections that would allow data transmission FROM the Internet to be received by the EMS server.

And the experts agree.

According to Barbara Simons, Ph.D., a former President of the Association for Computing Machinery, "It's a very bad idea to allow Internet access to an election management system." Such connections should never be confused with simply displaying election data on a website, which poses no risk.

And Dr. Doug Jones of the University of Iowa's Computer Science Dept. told us, "What we need is a prohibition on direct connections, or rather, a requirement that any connection to the Internet be in such a way that export of vote totals from the vote server is possible, while communication from the Internet to the vote tabulation system is impossible."

Dr. Mark Lindeman, who teaches political studies at Bard College in New York, offered this opinion on the importance of audits, "An election audit is supposed to bolster confidence that the winner actually won. If an audit protocol doesn't assure a high probability of detecting outcome-altering miscount, it will break down just when the public is paying most attention." Lindeman has independently confirmed both published and unpublished work by several authors showing that such audits are entirely feasible for all federal elections.

Furthermore, it should be self-evident that any instructions to voters to check VVPARs must be provided in multiple languages, made accessible to the disabled, and be placed in close proximity to each DRE or electronic ballot marker (EBM) wherever DREs or EBMs are used. Not doing so would violate equal protection under the law as well as HAVA's Accessibility requirements.

We believe that anyone with a bona fide interest in election integrity should be on the lookout for the above loopholes (and others too numerous to mention) in any current or proposed legislation and must fight to close them before it's too late.

Howard Stanislevic is a computer network engineer with over 25 years experience who has worked with the Internet Engineering Task Force.

John Washburn has been a software test professional for 12 years and a software developer for the 10 years prior. He has held the Certified Software Quality Engineer certification from ASQ since 1998.