Iowans for Voting Integrity

California's Report on Diebold: Important Findings

- An issue of trust: Diebold has asserted that they fixed some of these issues years ago. They have not.[1]

- Even a good chain of custody is not enough: "*...because the Diebold system is* ***vulnerable in so many ways****, the procedures required to protect it would likely be extensive, complex, and hard to follow. Hence, we worry that despite the best efforts and intentions of election officials, the system would sometimes be left open to attack*."[2]

- The programming skill and technical knowledge necessary to create malicious code for Diebold equipment are "likely available on the black market."[3]

- A person with even a few moments physical access to a single voting machine could load malicious software that infects the machine, and then the GEMS (Global Election Management System) server. Once GEMS is infected, every voting machine in a county could be compromised.[4]

- Anyone with access to the GEMS election management server could permanently load malicious software that, even if discovered, would be "very difficult to disinfect with confidence."[5]

- Modem and network communication between the election management server and the voting machines can be hacked, introducing "virally propagating malicious code into the server," and infecting all the voting machine in the county in the next election.[6]

- The GEMS server and the TSX do not provide a way for election officials to verify whether software on the machines has been modified.[7]

- GEMS audit logs can be subverted, allowing a user to conceal actions taken while logged in. [8]

- An administrative user of GEMS could change the user ID under which he or she was working.[9]

- GEMS has a remotely accessible Windows account that is not mentioned by name in Diebold's

---

[1] Edward Felten, professory of computer science and director of the Center for Information Technology Policy at Princeton University, http://www.freedom-to-tinker.com/?p=1184#comments)

[2] David Wagner and colleagues, "Source Code Review of the Diebold Voting System," p. 1. http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf

[3] "", p. 10

[4] Source Code review, p. 13

[5] Source Code review, p. 22

[6] "", p. 61.

[7] "", p. 22.

[8] Robert Abbott and colleagues, University of California Red Team report on Diebold Election Systems, p. 11. http://www.american.edu/ia/cfer/report/full_report.pdf

[9] Red Team report, p. 11

documentation, and which does not require a password for access.[10]

- GEMS runs on Windows software, which requires frequent patches. But updates and patches are themselves a point of attack that can introduce malicious code.[11]

- A "very low-skilled attacker" could, from a touch screen voting machine, escalate the privileges to those of a GEMS administrator.[12]

- A number of previously reported and "highly exploitable" bugs on the Accu-Vote ballot scanner remain in its software[13].

- The TSX touchscreen compromises ballot secrecy by storing votes with a timestamp.[14]

- Pre-election logic and accuracy testing offers little defense against software-based attacks; malicious software can recognize testing conditions.[15]

- Tamper-evident seals, upon which so much depends given the vulnerabilities of this system, have known vulnerabilities that can allow a person to break and then "restore them to a condition in which tampering is unlikely to be detected."[16]

- Diebold did not provide all of the code it has written for its voting systems, though this was a condition of the review.[17]

- What the report does not show: the review team did not review all of the code, or attempt to find any malicious code; source code analysis "cannot ensure that the equipment is free of security vulnerabilities or malicious logic designed to rig an election."[18]

- What the report *could* not show: it could not look for weaknesses in the source code for the unmodified commercial off the shelf (COTS) software (such as Windows or C libraries), in the Diebold system.[19] COTS software was exempt from the review and is exempt from any federal voting system testing. COTS software is a possible point of attack. The 2006 Brennan Center report: "COTS software writers, who may themselves be contractors or subcontractors of the original company that sold the COTS software to the voting system vendor, are in a very good position to insert an attack program."[20]

- **No matter how secure a county election office is**, vendor insiders (and insiders at their contractors and subcontractors) will always be a major point of concern, as they write the software, and often program ballots and provide technical support to counties. [21] The bipartisan

---

10 "", p. 12

11 "The Machinery of Democracy: Protecting Elections in an Electronic World," Brennan Center Task Force on Voting System Security, June 2006, p. 35. http://brennancenter.org/dynamic/subpages/download_file_39288.pdf

12 "", p. 13

13 Source Code review, p. 32

14 "", p. 50

15 "", p. 58

16 "", p. 59

17 "", p. 4

18 David Wagner, Testimony on Source Code Disclosure to the House Administration Elections Subcommittee, March 15, 2007. http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2327&Itemid=26

19 Source Code review, p. 4

20 "The Machinery of Democracy," (the Brennan Center report), pp. 34-35

21 Source Code review, p.73

Carter-Baker Commission noted wisely in 2005: "*There is no reason to trust insiders in the election industry more than in other industries, such as gambling, where* ***sophisticated insider fraud has occurred despite extraordinary measures to prevent it.***"[22]

- Even if future systems improve on Diebold's security, "*All computer systems are subject to subtle errors. Moreover, computer systems can be deliberately corrupted at any stage of their design, manufacture, and use. The methods used to do this can be extremely difficult to foresee and detect.* "[23] **Voters and governments will always have to "trust, but verify."**

[22] "Building Confidence in U.S. Election: Report of the Commission on Federal Election Reform," p. 28 http://www.american.edu/ia/cfer/report/full_report.pdf

[23] "Resolution on Electronic Voting." This resolution was endorsed by over 2000 computer scientists (including the most respected in the field), programmers, systems engineers. http://www.verifiedvotingfoundation.org/article.php?id=5028