Florida State University

Statement of Work

Title

Software Review and Security Analysis for
ES&S iVotronic Voting Machine Firmware.

December 15, 2006

Abstract

Florida State University is to conduct an independent software code review and security analysis of ES&S iVotronic voting machines as used in Sarasota County, Florida for the 13th U.S. Congressional District race during the 2006 General Election. This review is to provide information to the Florida Department of State relating to the higher than expected under-vote in that race.

Project Description

1. Introduction.

The Florida State University (hereinafter "FSU") shall act as an agent and on behalf of the Florida Department of State/Division of Elections (hereinafter "DOS") to assist DOS in the performance of its authority and duty in sections 101.58 and 101.5607, Florida Statutes. FSU shall conduct an independent software review and security analysis of the ES&S (hereinafter "the Vendor) iVotronic voting machine firmware used in the Florida 13th U.S. Congressional District race in the 2006 General Election conducted in Sarasota County (hereinafter "The District 13 Race"). This review is for the purpose of yielding technological data to DOS as relates to the higher than expected under-vote in the District 13 Race.

2. Project Scope and Organization.

The sole purpose of this project is to conduct a scientifically rigorous static software analysis on the iVotronics version 8.0.1.2 firmware source code to determine and identify flaws, vulnerabilities or anomalies, if any, that may have potentially caused, contributed or otherwise created the higher than expected under-vote rate in the District 13 Race. The project team for FSU shall exercise well-known software analysis techniques at their scientific discretion including code walkthrough, automated code scanning, debuggers, and other techniques including but not limited to those documented in Section 5.

3. Project Structure.

FSU shall act through a project team as designated in section 4.2 and hereinafter referred to as the "FSU Project Team"), shall conduct its scientific software review and security analysis independently of DOS, the Vendor, and any third party. The lead Principle Investigator for the FSU Project Team shall coordinate its activities. The FSU Project Team, however, may upon its discretion, communicate and exchange communications as needed with the designated representatives for DOS and Vendor.

4. Project Plan.

DOS shall provide the FSU Project Team with a copy of the iVotronics Version 8.0.1.2 firmware source code which is and shall remain protected from public disclosure as a trade secret pursuant to the Florida Public Records law. Within 5 days of receipt of this source code, the FSU Project Team shall provide DOS with a project plan consistent with and solely for the purpose stated in Section 2. The project plan shall include a projected timeline, milestones, deliverables, and estimated cost based on the source

code volume, complexity of the review, and estimation metrics. The final projected timeline, estimated variation range and cost are subject to DOS approval.

Notwithstanding section 4.2, the project plan shall also include a plan for staffing with the names and titles of all persons who shall be involved, providing technical assistance, consulting service or otherwise contributing to this project. Tasks performed under this project shall be assigned exclusively to team members designated in accordance with Section 4.2.

4.1. Deliverables: Final Report.

4.1.1. The FSU Project Team shall conduct structured note-taking in parallel to the research activities in preparation for the final report, including daily documentation of any detected pertinent flaws. For purposes of this project, a pertinent flaw is a flaw, vulnerability or anomaly that the FSU Project Team has scientifically established as having possibly caused, contributed or otherwise created the higher than expected under-vote rate in the District 13 Race. The daily written observations shall include an identifier, the nature of the pertinent flaw, its effect, prerequisite conditions if any exist, and the process that revealed the pertinent flaw. These daily observations shall serve in part as the basis for the final report.

If during the course of its project review and analysis, the FSU Project Team detects or identifies non-pertinent or incidental flaws, whether actual or perceived, that fall outside the scope of this project review, the FSU Project Team shall notify DOS immediately.

4.1.2 The FSU Project Team shall prepare and produce a Final Report. Report generation shall consist of a four step process:

Step 1. The Team shall accumulate daily observations, draft its process summary, formulate and document its review, conclusions and findings, and consolidate these into the final report draft.

Step 2. The Team shall forward the draft final report to DOS for an opportunity to review, comment or otherwise provide feedback. The Team may adjust the final report to reflect feedback from DOS.

Step 3. The FSU Project Team shall finalize the report to include its conclusions and findings.

Step 4. The FSU Project Team shall provide the final report to DOS who shall be solely responsible for the initial public release of the report. Except as required by court order or procedure, or by law, the FSU Project Team shall not make or release any comments or other information about the final report to any third party via any medium for 45 days from the date of submission of the final report to DOS or until the final report is released by DOS, whichever is sooner.

4.2. FSU Project Team: Staff.

The FSU Project Team shall consist of experts and professionals as set forth below. Such project team staff, regardless of the employment relationship to FSU, are acting at the behest of FSU and thus are bound by the same terms and conditions as FSU who is acting as an agent and behalf of DOS. Due to the

nature and duration of the review, the FSU Project Team expects that the staff composition may be dynamic. Not all members will work directly on the target code, and the Team may divide into two or more teams when appropriate. The following members shall comprise the initial team of the principal investigators:

Alec Yasinsac, Associate Professor, Computer Science Department, Florida State University
Mike Burmester, Professor, Computer Science Department, Florida State University
Breno de Medeiros, Assistant Professor, Computer Science Department, Florida State University
Ed Felten, Professor, Computer Science Department, Princeton University
Michael Shamos, Professor Computer Science Department, Carnegie-Mellon University
David Wagner, Associate Professor, Computer Science Division, University of California-Berkley
Matt Bishop, Associate Professor, Department of Computer Science, University of California-Davis

The FSU Project Team may also include senior personnel, graduate students, and technical support staff designated by the lead Principal Investigator. Subject to approval by DOS, the FSU Project Team may designate any other persons (other than those already named) who are not faculty, staff, employees, students, personnel, or otherwise affiliated with FSU to participate in this project review and analysis. However, in order to ensure objectivity and independent review of such persons, the lead Principal Investigator must have team members Drs. Felton, Bishop, Shamos and Wagner who are not faculty FSU and any staff thereto, and any other participants subsequently designated execute a Certificate of Non-Conflict of Interest (Attachment "A"). Such Certificate shall remain in effect for the duration of the project even in the event of resignation or termination of the member or participant from the FSU Project Team.

DOS retains the right to designate its own staff or employees to observe as non-participating members at any time during the project review and analysis. Such designated DOS staff or employee(s) shall have access to all premises, records, equipment and members of the FSU Project Team.

5. Software Review.

The FSU Project Team shall conduct a thorough review of the software using well-known techniques and by applying uniquely acquired knowledge and skills as software and security experts and professionals. The following are representative of the tools the team will use:

5.1. <u>Programming environments</u>

* Microsoft Visual C
* Emacs

5.2. <u>Debuggers that allow</u>

* Statement by statement step execution

* Breakpoint execution
* Dynamic core memory review
* Execution Path analysis
* Data definition-use analysis
* Dynamic core memory modification
* Condition testing
* Boundary value analysis
* Entry point identification

Tools to support this analysis include the downloadable software “LXR cross referencer”.

5.3. Automated Software to detect well-known vulnerabilities such as

* Buffer-overflows.
* Dead code
* Race conditions
* Numeric overflows
* Other well-known vulnerabilities

Possible shrink-wrap tools include Coverity Prevent, Klockwork K7, and Code Sonar.

5.4. Design Construction tools

* Display code structure
* Data/function connections

5.5. Software Complexity metrics tools that measure

* Branch counts
* Number of modules
* Cohesion/coupling level
* Function points
* Number of distinct operators
* Number of operator occurrences
* Number of distinct operands
* Number of operand occurrences

5.6. Source Code Security Analyzers, such as Fortify SCA

5.7. Custom Tools.

During the course of the investigation, the FSU Project Team will inevitably encounter circumstances that require custom software to illuminate module functionality, clarify cause and effect, or to understand complex software operation.

6. Security.

The project review and analysis hereinunder shall be conducted onsite in a secured location at the Security and Assurance in Information Technology (SAIT) Labs at Florida State University. Such project review and analysis shall be conducted in accordance with the General Security Precautions (hereinafter Attachment "B") and Project Security Management Plan (hereinafter Attachment "C"), both of which are incorporated by reference as if set forth in its entirety, and with FSU's established standards and protocols for ensuring the security and integrity of information technology, sensitive data, equipment, and physical facility.

7. Research Resources Including Data, Information, Records, and Equipment.

During the project review and analysis, communications are limited to the FSU Project Team who may interact personally or electronically among themselves, with DOS or the Vendor as it deems appropriate and may consult whatever resources are available including publicly available documentation via the Internet.

DOS shall provide the FSU Project Team with all the pertinent information and records that are required to be filed with DOS under section 101.5607, Florida Statutes, as relates to the certified ES&S iVotronic voting system that are necessary for purposes of conducting the software review and security analysis. The documentation shall include the voting system qualification report on such system for software testing by the designated Independent Testing Authority which is not a prerequisite for Florida Certification but if conducted, is required to be submitted as part of the application for certification under Florida law. All information and records provided to the FSU Project Team shall be documented and shall not be removed from the designated secure location.

The FSU Project Team may request technical and non-technical assistance, additional information and other resources available from the Vendor's designated representative to obtain that which is solely necessary to conduct the software review and security analysis including the information underlying the basis for the ITA qualification report.

8. Public Records Law

As an agent of DOS for the sole purpose of this software review and security analysis, FSU is bound by the same terms and conditions under which DOS is obligated under applicable federal and state statutes and rules to maintain or protect from disclosure information, records and data that are confidential and exempt from public access as trade secrets.

No information, record or data which is provided or accessed that directly pertains or exclusively relates to the project review and analysis or that is not already available in the public domain shall be discussed, published, disclosed, transferred or otherwise communicated outside the scope of the project review and analysis. No documents, files, papers, records, computer disks, or other tangible matters

containing data, files or records shall be removed from the secured location without express written permission of the lead Principal Investigator of the FSU Project Team, and in a manner consistent with section 3 of Attachment C. The lead Principal Investigator of the FSU Project Team shall be responsible for requiring all members of the FSU Project Team including non-FSU participants and their staff to execute acknowledgments that they have read, understood and agreed to abide by the terms and conditions of this Statement of Work. See Acknowledgement, Attachment "D." Such executed acknowledgement shall remain in effect for the duration of the project even in the event of resignation or termination of the member or participant from the FSU Project Team. Upon completion of the final report, all information, data, and documentation, original and copies, provided by DOS to FSU shall be returned promptly to the attention of David Drury, Chief, Bureau of Voting System Certification, Florida Department of State, R.A. Gray Building, 500 S. Bronough Street, Tallahassee, Florida 32399.

9. Conclusion and Matters not Covered.

If a matter or issue is encountered during this project review that is not covered by this Statement of Work the FSU Project Team shall notify DOS and as needed, the Vendor, for resolution.