Principal Investigator's Statement on Protection of Security-Sensitive Information

David Wagner
Principal Investigator
University of California, Berkeley

August 2, 2007

In May 2007, the California Secretary of State commissioned the University of California to conduct a security evaluation of the source code of several voting systems, as part of the Secretary's top-to-bottom review of these voting systems. As we prepared the final reports describing the findings from our source code review, we took great pains to ensure that our public reports would not inadvertently endanger the security of the country's elections. This note describes the approach we took.

In publicly discussing the security of any fielded system, there is often an inherent tension between our dual obligations as responsible engineers to precisely identify potential weaknesses and also to avoid aiding those who might seek to exploit them. These obligations themselves are closely intertwined, ultimately serving the common goal of making our society less vulnerable to the misconduct of criminals. Flaws cannot be fixed if they are not properly understood, and the modern history of technology repeatedly reminds us that we rely on the presumed ignorance of attackers only at great peril.

A common, widely accepted practice in the security literature is to describe attacks in sufficient detail to allow others to independently reproduce and evaluate the threat and, ultimately, build systems that better resist attack. Because of the severity of the attacks we found, and because we wanted to avoid making it easy for would-be attackers to subvert elections, we did not follow that practice here.

Instead, in preparing our public reports, we deliberately chose to err on the side of caution. We carefully screened all of the information that we included in our public reports. Our objective was to avoid reducing the amount of access an attacker would require to attack elections. We attempted to accomplish this by omitting details that would have the effect of converting an attack that would require reverse engineering or access to the source code into one that would not. These details were relegated to a confidential appendix provided to the Secretary of State. In some cases we deviated from this guideline when an attack scenario was already readily obvious from the interfaces presented to the user or from the previously published literature.

Our final reports are not intended to provide the level of technical detail that is typically expected in scientific publications. Reproducibility is at the heart of the scientific enterprise, and scientific standards generally dictate that technical data be fully disclosed to enable other scientists to independently reproduce the results. However, because we specifically wanted to avoid making it easy for would-be attackers to reproduce these attack scenarios in actual elections, our public reports omit certain technical information that would otherwise be expected under scientific norms. We recognize that independent scientists who seek to reproduce our results with the aim of building more robust systems may find the omissions frustrating.

In the end, our reports strike a careful balance between the public's interest in transparency into whether their voting systems are secure and the public's interest in being protected against the risks due to the disclosure of those flaws. We hope that future voting systems, better engineered than today's systems, will eliminate the need for such trade-offs.