On December 14th, 2007, Ohio Secretary of State Jennifer Brunner released the results of a comprehensive review of her state's electronic voting technology. The study, called *Project EVEREST,* examined electronic voting systems – touch-screen and optical scan – from Elections Systems and Software (ES&S), Hart InterCivic, and Premier Election Systems (formerly Diebold). As part of that study, three teams of security researchers, based at Pennsylvania State University (State College, PA), the University of Pennsylvania (Philadelphia, PA), and WebWise Security, Inc. (Santa Barbara, CA), conducted the security reviews. The reviews began in September, 2007 and concluded on December 7, 2007 with the delivery of the final report. The teams had access to voting machines and software source code from the three vendors, and performed source code analysis and security penetration testing with the aim of identifying security problems that might affect the integrity of elections that use the equipment.

Our report is an extensive technical analysis of the security of these voting systems as they would be used under real-world election conditions. All of our findings are detailed in this public report. A confidential unredacted version of the report provides specific references to the vendors' proprietary source code, but offers no substantive additional technical insights. The public report can be downloaded from:

`http://www.sos.state.oh.us/sos/info/everest.aspx`

Our study identified exploitable security weaknesses in all three vendors' systems. Many of these vulnerabilities represent practical threats to the integrity of elections as they are conducted in Ohio.

While some of the technical weaknesses we identified can be mitigated with improved procedural safeguards, others are more systemic. These structural flaws are more more difficult to correct, and reliably correcting them will require re-engineering and redesign of the equipment and software itself.

The security failures themselves could affect the entirety of the election process. We found vulnerabilities in different vendor systems that would, for example, allow voters and poll-workers to place multiple votes, to infect the precinct with virus software, or to corrupt previously cast votes–sometimes irrevocably. Further problems persist at the election headquarters, where election software running on commodity Microsoft Windows 2000 or XP machines could be compromised by viruses arriving from precincts, or by an attacker with seconds at the controller terminal. These latter security failures could expose precinct or county-wide ballots and tallies to widespread manipulation.

Two characteristics of the all of the vendor systems emerged from our analysis bear further comment. First, the systems exhibited a near universal lack of effective protections against insiders. Unmonitored poll-workers and election officials could exploit security failures to circumvent protections or misuse software features to manipulate voting equipment, vote counts, and audit information. Second, there was a pervasive lack of quality in the implementation (coding and manufacturing) of these systems. Failures were present in almost every device and software module we investigated. Such problems may lead to serious stability issues, and are the source of many security issues.

Our review concludes that the vendor systems lack basic technical protections necessary to guarantee a trustworthy election. Thus, we strongly believe that the integrity of the election relies almost entirely on the physical procedures used to carry out the election. We further conclude that some weaknesses are of a depth and magnitude that formulating reliable and workable procedural safeguards will be a very difficult task.

The review teams at Pennsylvania State University: Kevin Butler, William Enck, Harri Hursti, Steve McLaughlin and Patrick Traynor at the Pennsylvania State University. At the University of Pennsylvania: Adam Aviv, Pavol Černý, Sandy Clark, Eric Cronin, Gaurav Shah, and Micah Sherr. At WebWise Security, Inc: Richard Kemmerer, Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, William Robertson, and Fredrik Valeur. Elections legal and procedural consultants: Joseph Lorenzo Hall and Laura Quilter.

Patrick McDaniel, *Principal Investigator and Team Leader–Pennsylvania State University*
Matt Blaze, *Team Leader–University of Pennsylvania*
Giovanni Vigna, *Team Leader–WebWise Security, Inc.*