Evaluation of Elections Systems & Software (ES&S) Voting Equipment

On December 7, 2007, the Ohio Secretary of State released a report (EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing) found at http://www.sos.state.oh.us/sos/info/EVEREST/14-AcademicFinalEVERESTReport.pdf

This report was prepared for the Secretary of State by teams from the Pennsylvania State University, the University of Pennsylvania, and WebWise Security, Inc. Part II, consisting of Chapters 4 – 9, pages 27-99, contains an analysis of Elections Systems and Software (ES&S) voting machines.

In South Carolina, the ES&S voting systems include iVotronic direct recording electronic touch-screen voting machines, a Unity computer for each county, and Model 650 and Model 100 optical scan machines. A major difference between machines used in South Carolina and those tested in Ohio is that iVotronics in Ohio have an add-on paper tape, where the vote cast is recorded for use in a recount. This paper tape (called a Real Time Audit Log or RTAL) records the votes sequentially, making it possible to associate particular ballots with individual voters. The iVotronics used in South Carolina do not have this paper tape and in South Carolina there is no voter-verified paper record of the voter's intention.

Although election procedures may be different in the two states, the equipment used is very similar and subject to many of the same problems. Problems were found with every component of the system.

The following quote is from page 29: "Our analysis suggests that the ES&S Unity EMS, iVotronic DRE and M100 optical scan systems lack the fundamental technical controls necessary to guarantee a trustworthy election under operational conditions. Exploitable vulnerabilities allow even persons with limited access – voters and precinct poll workers – to compromise voting machines and precinct results, and, in some cases, to inject and spread software viruses into the central election management system. Such compromises render the election result subject to subtle manipulations – potentially across election cycles. These vulnerabilities arise from several pervasive, critical failures of the ES&S system:"

The Executive Summary of flaws in ES&S equipment lists the following four failures:

"*Failure to protect election data and software* -- … Virtually every piece of critical data at a precinct – including precinct vote tallies, equipment configuration and equipment firmware – can be compromised through exposed interfaces, without knowledge of passwords and without the use of specialized proprietary hardware.

"*Failure to effectively control access to elections operations* – … For example undocumented 'quality assurance' hardware tokens that bypass password checks are easily forged using inexpensive commodity devices such as palmtop computers. …

"*Failure to correctly implement security mechanisms* – Many of the most serious vulnerabilities in the ES&S system arise from the incorrect use of security technologies such as cryptography. This effectively neutralizes several basic security features, exposing the system and its data to misuse or manipulation.

"*Failure to follow standard software and security engineering practices* -- … Examples of poor or unsafe coding practices, unclear or undefined security goals, technology misuse, and poor maintenance are pervasive. This general lack of quality leads to a buggy, unstable, and exploitable system."

On page 30, in the Executive Summary: "The security failings of the ES&S system are severe and pervasive. There are exploitable weaknesses in virtually every election device and software module, and

we found practical attacks that can be mounted by almost any participant in an election. For this reason, the team feels strongly that any prudent approach to securing ES&S-based elections must include a substantial re-engineering of the software and firmware architecture to make it 'secure by design.'"

The Executive Summary concludes by suggesting that, in order to eliminate precinct-based attacks, it may be possible to use only centrally-counted optical scan hardware, but does not suggest how to do this.

Recommendations of the Ohio Secretary of State

The Secretary of State has recommended the elimination of the use of DREs (such as the iVotronic) and precinct-based optical scan voting machines that tabulate votes at poling locations. She has required that all ballots be optical scan ballots for central tabulation and effective voter verification. (This seems to imply printed paper ballots, to be counted at each county office.) For more information about these recommendations see

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

Selected Quotes from the Ohio Report

"Both the Unity tallying system and the iVotronic terminal have buffer overflow software bugs that allow an attacker who can provide input (e.g., on a PEB or memory card) to effectively take control over the system. … Avoiding buffer overflows in input processing is regarded as one of the most basic defenses a system must have.

"We found numerous buffer overflows throughout the ES&S system. Several of these buffer overflows – in the Unity tallying software and in the iVotronic terminal firmware – have extremely serious practical security implications. An attacker who can present input to any these systems (on an iVotronic PEB or on an M100 memory card from a precinct) can exercise complete control over the results reported by the entire county election system.

"Most seriously, the nature of these vulnerabilities means that there are few barriers to obtaining the access required to exploit them. In the case of the iVotronic system, voter access to the terminal is sufficient. In the case of the Unity system, brief access to any iVotronic or M100 optical scan results media returned back to the county for processing is sufficient.

"… there is a special Quality Assurance (QA) PEB type recognized by the iVotronic firmware that behaves essentially as a supervisor PEB but that, when used, does not require the entry of any passwords. … This undocumented PEB feature can be used to neutralize the security of any iVotronic administration features that depend on passwords …"

"…a voter can compromise an iVotronic terminal though its PEB slot. The iVotronic, then, may be programmed to create results media (at the end of the election day) that, in turn, corrupts the software of the central Unity system. The compromised Unity system, in turn, may be programmed to load corrupted firmware into all M100s and iVotronics in the county when provisioning a subsequent election. At this point, every major component of the system is running compromised code, which originated with a single attacker with only voter access in a single precinct. Needless to say, such an attack represents a grave threat to the integrity of the elections of any jurisdiction to which this happens."

"A voter who can emulate a PEB (by combining the attacks described in Sections 7.2.1 and 7.2.2) can use the PEB emulator (e.g., a Palm Pilot) to authorize multiple voter sessions."

“Approximately 63% of the source code is written using programming languages that are memory unsafe. These languages (C, C++, and assembly) allow several classes of vulnerabilities, including stack and heap overflows, integer overflows, and format string attacks. More modern programming languages (for example, Java and C#) are type safe and are not susceptible to such memory violations, and are therefore sometimes favored when developing security-critical applications. Although techniques exist for annotating C code (comprising roughly 23% of the ES&S source code) to achieve type safety, such approaches were not utilized.”

“ES&S makes use of third-party software, including the Windows and QNX operating systems, Compact-Flash device drivers, and PCMCIA flash device drivers. Although such software is useful for rapid software development, it is difficult to analyze the security properties of closed-source third-party systems. Without access to the source code or a time-consuming analysis of the third party software’s binary objects, these third-party systems are used as “black boxes” under the (possibly incorrect) assumption that they are secure. Since any vulnerability in a third-party product is automatically inherited by the system using it, such trust is unwarranted for security conscious applications.”

From Section 6.5, page 58:

“We believe the issues reported in this study represent practical threats to ES&S-based elections as they are conducted in Ohio. It may in some cases be possible to construct procedural safeguards that partially mitigate some of the individual vulnerabilities. However, taken as a whole, the security failures in the ES&S system are of a magnitude and depth that, absent a substantial re-engineering of the software itself, renders procedural changes alone unlikely to meaningfully improve security.

“Nevertheless, we attempted to identify practical procedural safeguards that might substantially increase the security of the ES&S system in practice. We regret that we ultimately failed to find any such procedures that we could recommend with any degree of confidence.

“A particular challenge in securing systems that use the iVotronic DRE terminal is the large number of precinct-based attack vectors whose exploitation must be prevented. Effective procedures that accomplish this, even if they existed, would be arduous indeed, and would likely substantially hamper poll workers in their duties, reduce the ability to serve voters efficiently, and greatly increase the logistical challenges of running an election.

“It may be possible to deploy a reduced subset of the ES&S hardware and software that excludes components that present the greatest risks. For example, a system that uses only centrally-counted optical scan hardware eliminates many of the threats of precinct-based attacks. We defer to the expertise of the Ohio election officials to determine whether it is possible to use a version of the ES&S system with reduced functionality in a way that presents an acceptable level of risk to the integrity of their elections.”