

Secure Electronic Voting: A Challenge Ahead

Executive Insight Series

by Jonathan G. Gossels

Introduction

In response to the vote counting problems in the 2000 presidential election, the Help America Vote Act (HAVA) was passed on October 2002. With funds available from that bill, approximately 675 counties have purchased touch screen voting systems known as Direct Recording Electronic (“DRE”) voting systems, to replace their existing voting machines. These 675 counties account for approximately 30 percent of registered voters in the country.

While the current DRE technology appears to offer greater accessibility to voters with disabilities and theoretically lower rates of lost votes, these machines have been documented to have critical security problems and are susceptible to malfunction. Either circumstance could call into question the validity of election results. For example, one independent test of the AccuVote-TS terminal conducted by RABA Technologies demonstrated that an attacker can overwrite both the results file and the audit file on both the internal memory and the PCMCIA card thereby completely overwriting the results from that voting terminal.

That same test also demonstrated the ability to switch two candidates and still successfully load the election and ballot. A voter using this compromised terminal would appear to have voted for his candidate of choice but the vote would actually have been counted for another candidate.

To address these problems, civil rights advocates have championed the use of voter verified paper trails (VVPT) to provide a means of auditing touch screen systems.

However, even if voter verified paper trails become a requirement, systems cannot be upgraded in time for the November presidential election. States will need to take other measures to ensure the accuracy and integrity of votes cast using the existing DRE machines.

In June, 2004, the Brennan Center for Justice and the Leadership Conference on Civil Rights released a set of recommendations for improving the security of DRE Voting Machines. These recommendations were developed by a team of independent experts that drew extensively on SystemExperts’s long experience in securing high value systems. Numerous reports of flaws in DRE systems and concern about the impact of security breaches and simple malfunctions on the overall integrity of the November 2004 elections motivated this effort. These practical recommendations have received wide spread support (http://www.brennancenter.org/programs/downloads/voting_systems_final_recommendations.pdf).

What You Can Do

As a concerned citizen, you should ensure that your state and local voting officials are aware of the well documented security problems with the

current generation of DRE machine and that they need to establish appropriate procedures and compensating controls to ensure an accurate vote. Beyond that, you should insist that your voting officials implement the report’s recommendations including at a minimum:

- Using qualified professionals to assess the security of the DRE environment and its supporting procedures
- Correcting any problems found during the security assessment
- Establishing a permanent independent technology governance panel
- Developing training programs for all elections officials and workers on security procedures
- Preparing standardized procedures for response to alleged or actual security incidents

Final Word

Accurate voting is not a partisan issue. We all lose when the results of an election cannot be trusted and it is impossible to tell whether a locale’s tally reflects actual counted votes or simply a preprogrammed result.

The recommendations contained in the Brennan Center for Justice and the Leadership Conference on Civil Rights report simply make sense and should be implemented by any jurisdiction using the current DRE systems.

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and Windows security at USENIX, Networld-Interop, CSI, and InternetWorld are among the highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio. Every single full-time staff member is certified in some critical security area.

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients. www.systemexperts.com/services.html

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. We can perform "White Hat" penetration testing, web application vulnerability assessments, dial exposure ("war-dialing") reviews, firewall analysis, host hardening analysis, IP services inventorying, wireless LAN inventory, VPN assessments, and denial of service reviews to name some of the more frequent testing we do.

Security Blanket, Emergency Response & Incident Response "Scrimmage"

It is not a question of *if* your organization will be the target of a hacker; it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment. We can also help you prepare for these inevitable events by practicing your response through our acclaimed Incident Response "Scrimmage" Training Exercise.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest intrusion, firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in Windows, UNIX, and other heterogeneous environments. We also provide interim staffing up to the CISO level.

Interactive Security Workshops & Code Reviews

Using a highly interactive workshop style methodology, our consultants will work with your team to perform a quick but comprehensive review of the security of applications or systems in their full environmental and business context and help you to understand and apply industry best practices. You may use this as the jumping off point for planning and prioritizing security initiatives. Our clients value this Workshop approach because of the knowledge transfer that occurs – the discussions make their team better.

SystemExperts uses this Workshop methodology in a wide range of services including overall security architecture reviews, design reviews, compliance reviews such as CISP or ISO 17799 assessments, Application Service Provider (ASP) reviews, PeopleSoft security reviews, and security code reviews. In the case of code reviews, we perform the detailed analysis of security-critical code modules after completion of the on-site interactive assessment of the application's architecture.

Security Policy, Best Practices, & Strategy

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice. Over the past ten years, we have assisted some of the largest financial institutions in the world in developing overall security architectures.

Intrusion Detection & Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston Los Angeles New York San Francisco Tampa Washington DC
Sacramento

www.SystemExperts.com

info@SystemExperts.com