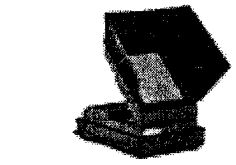
Response from Sequoia Voting Systems to the California Secretary of State's Office on the Top-To-Bottom Review of Voting Systems

Red Team and Accessibility Principal Investigator Reports on Sequoia's WinEDS version 3.1.012/Edge/Insight/400-C

Public Hearing~ Sacramento, CA
July 30, 2007



AVC Edge ®

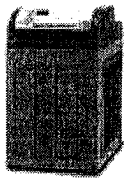
AVC Edge® with VeriVote Printer

AVC Advantage ®

This document is Sequoia Voting Systems' initial response to the California Secretary of State's office on the July 26th issued Red Team Penetration Testing and Accessibility portions of the Secretary's "Top-to-Bottom Review" of Sequoia's voting equipment currently used in 21 of California's 58 counties.

Nothing in life happens in isolation. As we have stated many times as have our nation's election officials, elections are a complex system made up of not only election equipment, but the people and the processes surrounding that equipment. California's Top-to-Bottom Review was not conducted in a true election environment or in accordance with ISO 15804, Common Criteria for Information Technology Security Evaluation and/or ISO/IEC 17799:2005. This was not a security risk evaluation but an unrealistic worst case scenario evaluation limited to malicious tests, studies and analysis performed in a laboratory environment by computer security experts with unfettered access to the machines and software over several weeks. This is not a real-world scenario and does not reflect the diligence, hard work and dedication to the stewardship of our nation's democracy that our customers - and all election officials - carry out every day in their very important jobs of conducting elections in California and throughout the United States.

As stated by our company many times in the past, with a Voter Verifiable Paper Audit Trail (VVPAT) that was pioneered by Sequoia in actual elections in 2004 and post-election checks that are already established by law and regulation, none of these attacks described in the Red Team report are capable of success. All would be prevented or detected through use of the VVPAT and legally sufficient audits. Red Team penetration testing is a well-known technique in the security industry. It is normally performed in a



Optech Insight ®

manner by which the system, in its native operation mode, is subjected to attacks from the Red Team, which is given various levels of knowledge regarding the system based on what the team is expected to emulate- insider threats, outsider threats, or ad hoc (a less defined test plan that can cross both insider and outsider threat boundaries).

In this case, the stated objective was to emulate both insider and outsider threats. However, the test plan actually employed suffers from misapplication of this methodology:

The Red Team had no corresponding Blue Team (friendly to the system under study) to emulate traditional and current election security practices. In short, the Red Team was able to, using a financial institution as an example, take away the locked front door of the bank branch, remove the security guard, remove the bank tellers, remove the panic alarm that notifies law enforcement, and have only slightly limited resources (particularly time and knowledge) to pick the lock on the bank vault. Such a scenario is implausible. Furthermore the equipment tested was not taken through the prescribed pre-election logic and accuracy testing and preparation, which would have included the addition of tamper evident seals. These seals, for example, would have precluded many of the attacks on the system.

The methodology used implies that election authority "insiders" have unlimited access to equipment, with no surveillance of their activities through automated methods. This is untrue. Election jurisdictions have several methods of insider deterrence and apprehension. These include cameras in the elections warehouse and computer rooms, audit logging on election database servers and workstations, and laws that make tampering with election equipment a felony at both state and national levels.

In summary, a more effective test would have been for the Red Team to have attacked a simulated target jurisdiction. Said jurisdiction would have prepared the equipment in keeping with traditional, current, and legally mandated equipment and procedural safeguards. The results of this test would have pointed out true weaknesses in election process security and provided real data from which governments could have improved their security profile. As it stands today, all that has been proven is that any computerized system, removed from its environment and placed, in this case almost literally, out in the street or into a laboratory for anyone to tamper with, can be successfully attacked. The data is thus unfortunately muddled by the inappropriate test methods, forcing governments to separate the wheat from the chaff of its ramifications for secure elections.

Sequoia will address each and every attack scenario in the Red Team report, its implications and mitigations as well as the points in the Accessibility Report.

In this presentation today, I will go through many of these points with you at a high-level summary and give some examples in the interest of our allotted time to present here today. We will share more information this week in response to both of these reports.

As for the Accessibility report, Sequoia's equipment complies with all requirements of the current 2002 VVSG as well as all California state requirements. Sequoia has worked with both national and local accessibility groups to design our voting system and we continue to do so in an effort to make all of our voting equipment as accessible as possible and continually improve our products as advances are made in technology to better assist persons with disabilities.

We appreciate some of the information and feedback contained in the Accessibility Report, however, many issues raised are not deficiencies in system design, but rather a function of the feedback we have received through national and local groups.

Going back to the Red Team Report, these described mitigations directly address each listed issue that the Red Team took with the Sequoia System. The mitigations fall within categories defined by ISO 27001, Information Security Management Systems. ISO 27001 is an international standard, valid in over 150 countries, for the protection of information and information systems. The ISO standard includes security practices around risk management personnel screening, computing network security, and business continuity/disaster recovery. Sequoia recommends that all governments involved in elections consider the ISO standard and its companion guidance document, ISO 17799-2005 when enhancing the security of their elections.

As an example of an issue we take with the Red Team Report, in the introductory portions of the report, the investigators define an "insider" and an "outsider" and note that "where system security relies upon proper application of procedures, it may be appropriate to examine the consequences of any failure to follow procedures." There are underlying automated systems (security cameras, server and client audit logging, etc.) that are present. The report takes none of these security systems into account in providing its results. Sequoia does concur that Red Team attackers should have knowledge of the system in order to simulate the patient or well-resourced attacker.

In section 3 of the Red Team report - "Known Issues" - the investigator describes the presence of "...known issues with the Sequoia voting system." Sequoia notes that these lists are unvalidated, and that when given a thorough investigation by the jurisdiction are found to lack merit and point not to the equipment or software, but to errors by pollworkers, issues brought about by distrust of the voting system, or other non-system related events.

In Section 3.1 of the Red Team Report, the Alameda County, California report is discussed. The Alameda County investigators recognized that any vulnerabilities identified could be and are mitigated by procedural mechanisms, as intended by the system. As such, they concluded that ¡°The Sequoia Electronic Voting System¡¡is inherently secure¡±. A few items copied into the Red Team report deserve comment:

- Item 1 - WinEDS and other services use non-encrypted test passwords when communicating. The current federally certified version (WinEDS

3.1.74) does encrypt all passwords. Furthermore, the version of WinEDS currently undergoing federal certification (4.0.0) has a completely new security access model which strictly controls access, passwords and the database itself at both the application and database levels.

- Item 2 - The Edge uses constant hashes and DES encryption keys as allowed by the current Voting Systems Standards. This portion of the system security scheme is in compliance with the required level of security. The risk of exploit is mitigated by restricting access to the machines in all areas, warehouse storage, preparation and use. The version of the Sequoia System which is being targeted for certification under the 2005 VVSG will implement a PKI methodology utilizing asymmetric key pairs and digital signatures to further improve security.

- Item 3 - Using cryptographic techniques will not prevent the results being copied across results media (in fact it is not desirable to prevent this due to operational aspects experienced by the jurisdictions) but will both prevent the results from being read and allow the results to be verified. The current approach is allowed by the current VVSG and therefore is compliant with the required level of security. Any risk is mitigated by restricting access to the machines and voting cartridges in all areas, warehouse storage, preparation and use. The version of the Sequoia System which is being targeted for certification under the 2005 VVSG will implement a PKI methodology utilizing asymmetric key pairs and digital signatures to further improve security.

- Item 4 - The WinEDS system uses Windows and therefore inherits the vulnerabilities associated with that operating system. As with most complex software systems, a common Commercial Off The Shelf (COTS) operating system is utilized - in this case Microsoft Windows. The risks associated with attacking vulnerabilities in the Windows operating system are mitigated with common procedural methods. Sequoia always recommends that the WinEDS server and clients are on an isolated network in a physically secure area. Even with this precaution, it is possible for malicious software to find its way into the network via results cartridges or other mobile data storage devices that may be used with the computers on the network. This is mitigated by ensuring a strict anti-virus and anti-spyware regime including that the most recent updates are utilized and heuristic functions included with the software are enabled.

In section 3.2 of the Red Team Report - "Multiple Votes Attack" - the investigator notes what has become known as "the yellow button attack." In this attack, the voter must reach around to the rear of the voting machine, past the privacy panels, find and actuate in a specific pattern the yellow activation button on the rear of the machine, without the notice of the pollworkers. This

attack is easily prevented by several means. The first is to disable activation through the yellow button through a configuration setting in WinEDS - the election management system. Secondly, numerous physical security measures can stop this attack. Placing the voting machines so that the rear of the machine faces the pollworkers aids in voter privacy and ensures that surreptitious attempts at repeated activation through the yellow button will be easily seen. Jurisdictions can also place a physical seal over the button to prevent it from being pressed until the authorized pollworkers remove the seal, using prescribed chain of custody procedures, and press the button.

The attacks outlined in sections 4.1 and 4.2 of the Red Team Report are example of ones that require unfettered access to the machines for a long period of time in a laboratory environment. It is extremely unlikely that anyone would be able to develop such an exploit when typical security measures are taken to restrict access to the machines. In many jurisdictions, units are stored in secure controlled areas where access to the units is controlled via electronic passes and access and movements are recorded on CCTV.

In section 4.3 of the Red Team Report - "Accuracy Testing Mode Detection" - the investigators could determine if a voting machine was in test mode or in Election Day mode. This is not surprising and is true of any system that provides a test mode of any sort. This opportunity to attack the system has been anticipated by both the vendor community and governments for many years and is the reason for Parallel Testing as required by the State of California. Parallel testing disables this attack and the State of California employs an excellent parallel testing program which serves as a model to election jurisdictions throughout the country.

Section 4.8 of the Red Team Report - "Security of the MS SQL Server" - points to the need for personnel security by the customer jurisdictions. As is true with any election system, whether touch-screen or paper based, some individual has access to the tally data. Persons with access to the central count server should undergo background checks commensurate with the valuable data that they maintain. Windows audit logging must be enabled, the allowable log size maximized, and the logs secured against accidental or intentional alteration or deletion. All of these practices are detailed in ISO 27001/ISO 17799 as described in the introduction of this document.

Section 4.10 of the Red Team Report - "Possible Unsafe OS Choices" - indicates the recommendations for use of Windows 98 or ME for client computers. This is due to the age of WinEDS 3.1.012, currently certified in the State of California. Newer federally certified WinEDS packages and their documentation call for use of Windows 2000 and XP, with their enhanced security profiles.

Section 4.11 of the Red Team Report - "Physical Security" - indicates that tamper evident seals are easily bypassed. While seals can be removed, as is their intended use, they cannot be removed undetectably. In cases where pollworker access is required to fulfill election responsibilities, tamper evident seals provide a convenient method to bring to the surface any attacks

on the equipment so that the equipment can be quarantined and the election continue without its results becoming suspect. Tamper evident seals have been used in military environments for many decades, and consist of adhesive tapes with unique identifiers, which can not be removed without breaking them. They could be placed on every access point, including access covers and chassis screws and a record kept of the numbers. Jurisdiction procedures would log that the unique identifiers on the tamper evident seals match established records to ensure that no equipment tampering had occurred.

Section 4.13 of the Red Team Report - "Forging Update Cards and Voter Cards" - is mitigated through physically securing the voting machines, election specific information on the voter card, and traditional and current pollworker training. This scenario requires that attackers gain access to the voting machines and could successfully extract and utilize the information regarding voter card programming. Not only this static information needs to be extracted, but the ballot style for a particular precinct would need to be known to the attacker in advance. Without valid ballot style information, which changes from election to election, this attack fails ¨C the voter card is rejected by the voting machine as invalid. Pollworkers are responsible for ensuring that only voters that have just received voter cards from them approach the machines. It is unreasonable to believe that a person or persons could approach the line of voting machines in a precinct without having been credentialed, and especially that an attacker or group of attackers could do so repeatedly.

Section 5 Attack Scenarios - While these attacks may have been successful given the uncontrolled environment of the investigation, they would not succeed in an actual election.

Attack scenario 1 (insert a malicious HAAT USB stick into the initialization process) relies on two assumptions: that there is a pool of HAAT USB sticks for initialization such that a malicious HAAT USB stick could be inserted into that pool; and autorun on the WinEDS computer is allowed. HAAT USB sticks are specific to each precinct or polling location, thus it would be extremely unlikely that a malicious USB stick could be inserted into the jurisdiction's HAAT initialization process. As stated above, autorun features should be disabled on all computers performing election related tasks.

Likewise, the assumption that a large number of voters do not check their vote on the paper record, when it scrolls in front of them (providing both visual and audible cues as to its existence) and when the voter is forced to interact with the voting machine to produce the record, is also false.

Sequoia always recommends that the WinEDS server and clients are on an isolated network in a physically secure area with strict access control. All mobile data storage devices should be checked for viruses and spyware on a stand alone computer before being introduced to the secure area. U3 flash drives should not be permitted in the secure area and should never be used on the system.

Even with these precautions, it is possible for malicious software to find its

way into the network via results cartridges or other mobile data storage devices that may be used with the computers on the network. This is mitigated by ensuring a strict Virus and Spyware detection regime is implemented on the system, including ensuring the most recent updates are utilized

Attack scenario 2 (same as attack scenario 1, but with a fleeing voter that did not review their paper ballot) is likewise implausible. How would the malicious software know that the voter had actually fled? The interaction with the voter and a pollworker is the same regardless of which one actually completes the ballot casting process. Pollworkers need to keep the voting machines open, so fleeing voters' ballots are typically cast quickly after the voter leaves the voting machine, so time intervals would not aid the malicious software in determining when it could successfully change a voter¡¯s ballot choices.

Attack scenarios 3 and 4 rely on the voter leaving the voting machine within a few seconds of the voting process ending, and the next voter not appearing at the machine long enough for the voting machine to print and obscure its VVPAT record. This is not plausible in the least. Voters, some carrying purses, children, and other items, will take several seconds to leave the booth, during which time any number of them would notice the odd behavior of the voting machine, and that it voided their VVPAT record. Some voters will leave the booth quickly. If the voter leaves the booth quickly, then the next voter is likely to see the voided paper record and either notify the previous voter or call a pollworker. Either of these actions calls attention to the errant machine behavior. An Edge VVPAT requires ten or more seconds to print a VVPAT page, so there is more than adequate time for voters to read the maliciously voided record and be alerted to the machine behavior.

Attack scenario 5 is easily thwarted with tamper evident seals and the scope of effort required to tamper with a statistically significant number of Edge units. It is implausible to successfully carry out this attack.

Attack scenario 6 regarding voter cards would require that attackers gain access to the voting machines and could successfully extract and utilize the information regarding voter card programming. The attacker also needs to determine the ballot style information that is valid at a particular precinct/polling location. If the card is programmed with no style information or incorrect style information the card will be rejected by the voting machine as invalid. Assuming an attack of this nature was attempted, pollworkers are responsible for ensuring that only voters that have just received voter cards from them approach the machines. They will notice if a person (or persons) enter multiple times and/or approach the machines without having received a voter card from them. Polling places are set up so that the voter must pass through a credentialing station prior to obtaining a voter card, and thus prior to approaching the voting machines. Traditional and current pollworker training and Election Day actions would prevent voters from voting multiple times. Voter cards are embossed with jurisdiction or Sequoia Voting Systems specific artwork so that volume purchases of blank voters cards could not be used successfully in an attack unless they were also forged with the

jurisdiction's artwork.

Attack scenario 7 regarding access to WinEDS and installation of malicious software fails with simple mitigations. Sequoia always recommends that the WinEDS server and clients are on an isolated network in a physically secure area with strict access control. Full MS-SQL security should be implemented, including encryption of passwords, and a strict and secure password management regime utilized.

The possibility of malicious software having found its way onto the network can be further mitigated by ensuring a strict anti-virus and anti-spyware regime is implemented on the system. This includes ensuring the most recent updates from Microsoft are tested then applied.

This type of attack is mitigated if, as described in the scenario, WinEDS is loaded on the server before each election is initialized, and just before Election Day. Further protection can be gained by taking digital signatures of the server after WinEDS installation and comparing them to hash values taken on Election Night. Procedures for loading software through trusted processes are published and practiced throughout various jurisdictions as well as industries outside of elections. Even in the extremely unlikely event that this sort of attack is attempted, the mitigations already discussed in relation to scenarios 1 through 4 would apply.

Potential Attack Scenario 8 regarding use of access to the 400C Central Count Optical Scanner to attack the tabulation of scanned ballots is also easily mitigated through the use of tamper evident seals. Sealing the compartment containing the 400C computer would allow for rapid detection of this attack, which could then be thwarted completely be re-installing the software on the 400C through trusted processes. Standard physical security practices such as electronic passes and surveillance would allow for identification of the attacker.

Conclusion

While this evaluation was an interesting and helpful theoretical exercise, it did not represent a security risk analysis and as such does not measure the severity of the actual threats in any meaningful way. The evaluation was limited to malicious tests, studies and analysis performed in a laboratory environment by computer security experts with unfettered access to the machines and software over several weeks. None of the traditional, statutory, or recommended security procedures were in place. This situation is unrealistic.

Sequoia concludes that none of the threats outlined represent a realistic threat if the normal, procedural mitigations are in effect. We are, however, entering the few system vulnerabilities found into our ISO 27001 compliant Corrective and Preventive Action System to further reduce opportunities for attackers. We are also considering the broader implications of each attack to refine our established recommendations to customers regarding system security.

Jurisdictions should consider conducting thorough security risk evaluations based on ISO 15804, Common Criteria for Information Technology Security Evaluation and/or ISO/IEC 17799:2005; and adopting security processes conforming to these international standards.

Lastly, the versions of the hardware, firmware and software systems evaluated were developed several years ago. While it can not be guaranteed that all of the extremely improbable vulnerabilities identified are prevented by subsequent product development and updates, many are specifically addressed.

Sequoia also believes that this evaluation identifies some potential weaknesses in the current VVSG, which have been addressed in later standards, and as such should the State believe that some of these threats outlined in the report are credible, it should consider purchasing new machines or updates to existing units that meet the 2005 VVSG, and subsequently adopt the 2007 VVSG when available.

On behalf of Sequoia Voting Systems, I would like to again thank Secretary Bowen and her staff for allowing Sequoia to participate in today¡¯s public hearing and comment on the Red Team and Accessibility reports. We look forward to working with Secretary Bowen, her staff and our customers this week and in the future as we go forward in providing secure, accurate and accessible election equipment for California voters.

CONTACT:
Michelle M. Shafer
Vice President of Communications
& External Affairs
Sequoia Voting Systems
800.347.4702
mshafer@sequoiavote.com