VoTeR Center
UConn Voting Technology Research Center
PI : A. Shvartsman, Ph.D.
Co-PIs: A. Kiayias Ph.D., L. Michel Ph.D., A. Russell Ph.D.

AccuVote Optical Scan Vulnerabilities and Safe Use

October 27, 2007

Version 0.1

Introduction

The development of modern computerized voting technology, while empowering voters, also introduces vulnerabilities due to the possibility of accidental or malicious interference with the voting processes. Recent reports have identified numerous such vulnerabilities. While it is difficult to provide absolute guarantees that proper operation of a particular voting terminal cannot be interfered with, in certain cases – once the vulnerabilities of the terminal is carefully assessed – it may be possible to design policies and procedures to be followed by the election workers so as to enable the safe use of the terminal by the voters and to ensure that the election results are correctly recorded.

The subject of this document is the AccuVote Optical Scan voting terminal (AV-OS). We begin by overviewing optical scan technology, contrasting it with the touch screen technology, and discussing the vulnerabilities issues of AV-OS terminals. We then explicitly enumerate the vulnerabilities identified for the AV-OS terminals and the impact of these vulnerabilities with respect to the possibility of malicious tampering with the vote counting and the election results. We conclude with the discussion of threat mitigation and recommendations for safe use of AV-OS terminals. The recommendations include imposing a strict chain-of-custody policy on AV-OS terminals and memory cards, pre-election testing of memory cards, and post-election audits.

Optical Scan Technology in Perspective

An important benefit of using the optical scan technology in electronic voting systems is that it naturally yields a voter-verified paper trail — the actual “bubble sheet” ballots

marked by the voters. This differentiates optical scan electronic voting from DRE (direct recording electronic) electronic voting terminals (such as the Premier's AccuVote TS and TSx terminals) that provide a digital interface for voting during the elections. We note that the current generation of the DRE terminals — especially paperless ones — have received substantial criticism due to a number of critical security vulnerabilities, such as those reported in [KSRW04, Hursti06, Princeton06, Berkeley06, UConn07]. Even when a DRE terminal is equipped with a printer, the computer-generated paper trail cannot be directly considered voter-verified, and it is possible for a faulty DRE to print spontaneous ballots while unobserved. Further development of the DRE technology is necessary for it to become a trustworthy alternative.

While optical scan voting is free from some of the perils of paperless trails or computer generated paper trails, the election still relies on the terminal to electronically add the votes and report the results; this introduces the possibility of attacks that interfere with these basic tabulation and reporting tasks. Such an attack against the AV-OS was demonstrated by Hursti [Hursti05]. This attack was particularly devastating as it initialized the counters of the terminal to negative or positive vote counts while still forcing the machine to report a valid zero-count initialization. This can lead to biased election results and corrupted election counts. The operation of the AV-OS system is in part governed by the instructions stored in a memory card that is inserted into the terminal for the duration of the election. The attack of [Hursti05] employed a memory card reader/writer to modify the card prior to election and bring it to an invalid initial state. When a maliciously altered card is used in an election, it records biased results that are successfully tabulated by the terminal. Given that the attack in [Hursti05] required tampering with the memory card directly, one way to mitigate the attack is to somehow ensure that the memory card stays in place sealed into the terminal throughout the period that the machine is in use or is in transit to and from the polling places. Alternatively (and most effectively) one could employ a cryptographic integrity check, however this would require modifications to the firmware of the system (presumably by the manufacturer). A second way to mitigate the attack would be to execute a pre-election test, hand-count the ballots, and compare this to the report of the terminal.

Given the facts summarized above, the pressing question was whether the security measures of (1) sealing the memory card into the terminal, and (2) performing pre-election testing with hand counted ballots, are sufficient to prevent an attack against an election employing the AV-OS.

Our own findings [UConn06] answer this question in the negative. In particular we showed that even if the memory card is sealed and pre-election testing is performed, one can carry out a devastating array of attacks against an election using only off-the-shelf equipment and without having ever to access the card physically or opening the AV-OS system box. Examples of our attacks include the following:

1. Neutralizing candidates. The votes cast for a candidate are not recorded.
2. Swapping candidates. The votes cast for two candidates are swapped.
3. Biased Reporting. The votes are counted correctly by the terminal, but they are reported incorrectly using conditionally-triggered biases.

Our attacks exploit the serial communication capability of the AV-OS and demonstrate how the attacker can easily take control of the machine and force it to compromise its sealed-in resident memory card. Moreover, we demonstrate how one can make the AV-OS appear to be uncompromised to an evaluator who performs a pre-election test by voting hand-counted ballots, or to an evaluator who examines the audit reports that are produced by the terminal. A corrupted terminal will in fact appear to be faithfully reporting any election procedure that is conducted prior to the day of the election, only to misreport its results on the day of the election.

The vulnerabilities documented in [UConn06] were developed by experimentation with the system. At no point in time had we used, or had access to, internal documentation from the manufacturer or the vendor, including internal machine specifications, source code of the machine's operating system, layout of the data on the memory card, or the source of the GEMS ballot design and tabulation software. We developed attacks and software that compromises the elections from first principles, by observing system's behavior and interaction with its environment. Based on this fact, we conclude that attackers with access to the components of the AV-OS system can reverse-engineer it in ways that critically compromise its security, discover the vulnerabilities presented herein and develop the attacks that exploit them.

Additional vulnerabilities are documented (the "Berkeley Report") by the members of the California Voting Technology Assessment Advisory Board (VSTAAB) with the assistance of the University of California, Berkeley, and issued on February 14, 2006 [Berkeley06]. The report documents a number of vulnerabilities due to the AccuBasic interpreter of the AV-OS and TSx voting terminals. What was discovered is that the implementation of the interpreter left the doors open for the election results to be tampered with by using some of the standard "hacking" techniques such as buffer overruns and array bound violations. These attacks can be devastating by leading to rogue code completely taking over the AV-OS system.

The vulnerabilities documented in the "Berkeley Report" complement both the "Hursti Attack" [Hursti05] and our findings [UConn06]. The "Berkeley Report" underscores the need for strict chain of custody of AV-OS, memory cards, and GEMS systems, and strong policies for who and how is to access these systems and devices. The report also lists several short- and longer-term mitigation strategies, all of which are clearly sensible, and should be implemented. Subsequent comprehensive reports in California [CA07] and Florida [FL07] confirm and catalog earlier findings.

Summary of Vulnerabilities

We now explicitly enumerate the vulnerabilities that exist in the AV-OS voting terminal as used in the State of Connecticut.

1. The AV-OS "leaks" the memory card contents: The AV-OS terminal allows any operator to obtain a dump of its installed memory card contents without any authentication control. In particular, given access to an AV-OS machine one can obtain all the information that is stored in the memory card in a matter of seconds. In order to obtain this information, it is sufficient to use an off-the-shelf RS-232 serial cable (null modem cable) and a laptop.
2. The AV-OS performs no authentication test to ensure that a trusted system is present on the other side while the dump is delivered in cleartext form. Moreover, the terminal does not prompt the operator for a password in order to produce such memory dump. It is easy to identify the election data when observing a memory dump; other sensitive information, including the password (PIN) and audit records associated with the memory card can also be reconstructed from the dump. Alternatively, the same dump can be obtained by using the built-in modem on the AV-OS to transmit the data to a remote PC.
3. The communication between AV-OS and GEMS is unauthenticated: During the initialization of a machine for election the GEMS system communicates with the AV-OS terminal to write the initial election setup to the memory card.
4. No encryption or cryptographic authentication is performed during this transmission. The serial line protocol does use a cyclic redundancy check (CRC) mechanism for error control. While the CRC polynomial used is standard, the details of the protocol are undocumented by the manufacturer; as such, this is a de facto lightweight authentication mechanism. However, it is possible to reverse-engineer the whole protocol, including the CRC scheme formula (as we have done in our assessment). The lack of cryptographic authentication opens the possibility for an unauthorized attacker computer to impersonate the GEMS system to the terminal.
5. Executable code within the AV-OS memory card: Each memory card contains executable code that is used for printing the reports. The code is written in a proprietary symbolic language. Such executable files are identified as .abo (AccuBasic Object) bytecode. The possibility to modify the code that prints the results opens the possibility to corrupt machines and coerce them into misinterpreting their counters. The presence of conditionals and arithmetic in the language enables bytecode "malware" to operate even conditionally on the state of the machine and thus appear to operate properly in some occasions while misreporting the results in others.
6. The AccuVote interpreter (residing in the firmware of the AV-OS terminal) is open to being corrupted by maliciously constructed .abo bytecode. This enables an

attacker to deliver malicious code through the memory card, resulting in arbitrary behavior of AV-OS during its deployment in an election.

7. AV-OS system does not check that valid firmware is contained in the PROM (read-only memory) chip. This in essence allows an attacker to load their own code in the AV-OS terminal that can result in arbitrary system behavior. This is a "hardware" attack that is more difficult to execute, but its consequence is identical to substituting a maliciously designed AV-OS look-alike terminal for a real terminal. (It is this "capability" that allows us to turn AV-OS into a memory card reader to speed-up dumping of the card contents for testing purposes.)

Impact of the Vulnerabilities

As the consequence of the vulnerabilities described above, AV-OS systems can be tampered with under the following circumstances.

1. Memory cards are accessed by unauthorized personnel after they are programmed and before they are inserted into AV-OS terminals.
2. AV-OS terminals are accessed by unauthorized personnel (with or without memory cards inserted).
3. AV-OS terminals are accessed by unauthorized personnel after memory cards inserted before an election deployment (whether or not the AV-OS have been tested with the inserted cards).

Additional Considerations

The printing of physical ballots is currently done as a separate process, only indirectly related to the programming of the GEMS database and subsequent loading of the election data into the memory cards. It is important to verify that the printed ballots indeed correspond to the election data contained in the memory cards. It is possible and advisable to construct test decks of ballots that explicitly check for correctness of printed ballots.

Finally, as we pointed out, the loading of the memory card from the GEMS system includes an executable program that is stored in the GEMS environment. It is also important to check that this program correctly deals with vote tabulation and printing, and that it does not include any extraneous, erroneous, or malicious code.

Threat Mitigation and Recommendations for Safe Use

Vulnerabilities such as the ones described above suggest the possibility of tampering with elections that can be exploited by a sophisticated attacker. Still, in many cases it can be possible to devise specific procedural and technological measures to successfully thwart

the attacks even without requiring any modification to a terminal. Thus, once a comprehensive listing of attack vectors against a voting terminal has been completed, it is possible to develop mitigation methodologies that may enable the safe use of a voting terminal in an election procedure despite the existence of vulnerabilities.

Given that the AV-OS terminal is merely a "bubble sheet" counting device and not a DRE system, there is no fear that the actual record of the decisions made by voters will be lost (since they are preserved in the voter generated paper trail). Nevertheless, the fact that the votes are not lost does not necessarily imply that they will be counted correctly. The attacks presented herein suggest that the AV-OS system has security defects in its design that demand strict observance of safe use guidelines. Based on our findings we propose the following.

1. It is important to seal in a tamper evident fashion not only the memory card slot but also the serial port and the phone jacks of the terminal. Instead of sealing these sockets it is possible to disconnect them internally from the motherboard so that they are disabled, although this approach has the disadvantage that its implementation cannot be verified without opening the system box.
2. Protecting the device with tamper-evident seals to secure it against opening of the system box is equally important. Opening the system box of the device not only makes the memory card exposed but also enables one to circumvent sealed serial ports by directly connecting a properly configured cable to the motherboard. Additionally this allows an attacker to replace the firmware chip. A complete approach involves protecting the entire AV-OS device within a tamper-evident enclosure at all times other than the actual deployment in an election. (This approach is being taken in Connecticut where the system carrying case is secured by a tamper-resistant numbered seal, with the seal number checked at all transit points.)
3. Chain of custody should be strictly observed, from the point of initialization of the terminal to the time it returns to long-term storage after an election. The procedures for transporting and handling the equipment must be defined in advance (such procedures are in place in Connecticut).
4. The memory card(s) must be stored in tamper-evident containers whenever it is outside the AV-OS terminal. Given that no cryptographic integrity check is employed by the AV-OS memory card management, the moment the election-ready card is stored in the open, or is removed from a terminal by unauthorized personnel, it can be considered to be compromised. Unfortunately even if the memory card is sealed in the terminal, as our attack demonstrated, the system does not guarantee an uncompromised election unless the remaining ports and case of the terminal are sealed in a tamper-evident fashion as well.
5. It is also necessary to safeguard the firmware chip in the AV-OS system. The chip contains the AccuBasic interpreter, and it is designed to be replaceable due to

version changes. It is imperative to ensure that the right chip is installed prior to the AV-OS machines being deployed for election.

6. Given that programmed memory cards are shipped to Connecticut from LHS Associates, it is important to verify that the received cards are indeed programmed correctly and that the received cards are indeed the cards that have been programmed per election data in GEMS system. This can be done by examining the memory cards upon their arrival in Connecticut. At least a random audit of the cards should be performed before the election.
7. Finally, a post-election random audits involving hand counting of the ballots are highly recommended. (Such random audits will be conducted in the State of Connecticut.) It is also advisable to perform post-election audits of the memory cards used in the elections.

Summary of Recommendations

The following procedures, once implemented, will substantially help ensuring the integrity of the use of AV-OS voting terminals in the elections in Connecticut.

- Implement strict chain-of-custody policy for AV-OS terminals.
- Implement strict chain-of-custody policy for memory cards.
- Implement pre-election testing of programmed memory cards.
- Implement post-election audits.

Additionally, it is important to ensure that the printed ballots correctly correspond to the election data programmed into the memory cards.

References

[Berkeley06] David Wagner, David Jefferson and Matt Bishop, Security Analysis of the Diebold AccuBasic Interpreter, Voting Systems Technology Assessment Advisory Board, University of California, Berkeley, February 14, 2006.

[CA07] California “Top-to-Bottom Review”, University of California, Berkeley, July 2007. http://www.sos.ca.gov/elections/elections_vsr.htm

[FL07] Florida “Software Review and Security Analysis of Diebold Voting Machine Software”, Florida State University, July 2007.

[Hursti05] Harri Hursti, Critical Security Issues with Diebold Optical Scan Design, Black Box Voting Project, July 4, 2005 http://www.blackboxvoting.org/BBVreport.pdf

[Hursti06] Harri Hursti, Diebold TSx Evaluation, Black Box Voting Project, May 11, 2006 http://www.blackboxvoting.org/BBVtsxstudy.pdf

[KSRW04] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan S. Wallach, Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy 2004, IEEE Computer Society Press, May 2004.

[Princeton06] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine, September 13, 2006 http://itpolicy.princeton.edu/voting

[UConn06] A. Kiayias, L. Michel, A. Russell, and A. A. Shvartsman. Security Assessment of the Diebold Optical Scan Voting Terminal, UConn Voting Technology Research Center, October 30, 2006, available at http://voter.engr.uconn.edu/voter/Reports.html.

[UConn07] A. Kiayias, L. Michel, A. Russell, and A. A. Shvartsman. Integrity Vulnerabilities in the Diebold TSX Voting Terminal. UConn Voting Technology Research Center, July 16, 2007, available at http://voter.engr.uconn.edu/voter/Reports.html.