InkaVote Plus
Red Team Security Penetration Test

for

California Secretary of State
Debra Bowen

2-7 October 2007

The Red Team security penetration test for the InkaVote Plus was conducted by

atsec information security
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

for California Secretary of State Debra Bowen under contract with Freeman, Craft, & McGregor Group (FCMG). atsec is accredited as a Common Criteria Evaluation Lab, a Cryptographic Module Test Lab (FIPS 140-2), and provides other computer security testing services for commercial companies.

General Description of Equipment Under Test (EUT)

The InkaVote Plus system, marketed by Election Systems & Software (ES&S), consists of the InkaVote Precinct Ballot Counter (PBC) and Unisyn Election Management System (EMS). The PBC is based on a standalone lottery ticket machine design developed by the International Lottery & Totalizator Systems, Inc. (ILTS). The system supports the InkaVote ballot which has been used in County of Los Angeles and City of Los Angeles elections for several years. The InkaVote ballot is a mark sense ballot based on the design of a Hollerith (IBM) punch card. Ballot identification data is pre-punched in the leading columns. To vote, the card is placed in a marking device which has a ballot voting booklet and template guide showing the location to mark a vote for each candidate in each contest. A special marking pen is used to mark the voter's choices. The InkaVote Plus PBC unit may be equipped with an optional component called the Audio Ballot unit which provides support to assist visually blind as well as other voters who need an audio ballot. The Audio Ballot unit consists of a keypad, earphones, and printer. This unit uses an audio ballot script which guides the voter through voting their choices and prints a marked InkaVote ballot. The voter may then insert the marked ballot into the PBC unit which checks for overvotes and blank ballots. Voters who mark their ballots manually or with the ballot booklet template may also use the PBC unit to check the ballots for overvotes and blank ballots. If an overvote or blank ballot is detected the system returns the ballot to the voter giving them an opportunity to remake the ballot. This error checking is a Help America Vote Act (HAVA) requirement. Although the

PBC unit is capable of tallying the ballots and producing a machine report of the results when the polls close, the City of Los Angeles and County of Los Angeles only use the system for the audio ballot and error checking functions without using the ballot tally and reporting functions. The InkaVote ballots are tallied and reports generated by a central counting system used for all the ballots, including both the polling place and absented ballots.

The Unisyn EMS suite of applications is a set of Java based software applications which allows the user to create election definitions for the PBC, load the election definition into one or more PBCs (multiple units may be programmed using an Ethernet link). The suite design includes the option to load compatible XML formatted election definitions from other election management systems. Once the polls close, the tally results may be transferred back to the EMS suite for accumulation of multiple PBCs' results and reporting. The Unisys EMS suite of applications operates on a Windows XP supported workstation. EMS component applications operate independently and may be installed on separate workstations as needed. They include:

- an election database, using MySQL;
- the application to modify and define the election for each election, which is identified in the manuals as the "EMS" application;
- an Election Converter which converts an XML description of an election and produces an encrypted Election CD;
- an Election Loader, which supports the installation of the election provided by the Election CD in each PBS using a local Ethernet network;
- a Vote Converter to transfer the voting results from the PBC using a USB memory media device as a carrier; and
- a Vote Tabulation module to tabulate, consolidate, and generate election reports on the voting results.

The County and city of Los Angeles provides the XML election definition from their legacy election system to the Election Converter component and uses the Election Loader component to load the election into the PBC. Because they do not use the tabulation and reporting capabilities of the system, the other components of EMS are not used.

Scope Limitations

The InkaVote system is being used only by Los Angeles County and the City of Los Angeles for the specific purposes of detecting and preventing the casting of ballots which are blank or have overvoted races and to provide the Audio Ballot interface to mark ballots for voters requiring the audio ballot. The ballot tabulation and reporting features of the InkaVote system are not being used in this venue. Accordingly, the examiners were asked to limit their examination, where possible, to the modules of the system which are being used by the County and City of Los Angeles and to vulnerabilities that effect:

- the integrity of the election definition needed to support the error detecting and Audio Ballot functions,
- security audit logs and the log reporting services, and
- the basic operation of the PBC (i.e. denial of service attacks).

The full system was supplied as a testing resource and all technical documentation was provided for reference. Components not in the scope of testing were open for review to the Red Team as a resource if needed. For example, during the Red Team test, the tally and report generation within the PBC were used to document and demonstrate the effectiveness of one of the demonstrated exploits. If the Red Team did notice that an identified vulnerability could affect vote tallies or reports, they were encouraged to report it although it was not a primary focus.

The County of Los Angeles processes to generate the XML were outside the scope of testing.

For the purpose of the test, the test team was asked to consider four classes of attackers:

- Voter: usually has low knowledge of the voting system machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine for less than one hour.
- Poll worker: Usually has a low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine for less than one day.
- Election official insider: Has a wide range of knowledge of the voting machine design and configuration. They may have restricted access for long periods of time. Their designated activities include:
    - Set up and pre-election procedures.
    - Election operation.
    - Post election processing of results, and
    - Archiving and storage operations.
- Vendor insider: Has a great knowledge of the voting system design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service, and when providing election administration services.

atsec added one other category on FCMG recommendation, the storage or warehouse worker with virtually unlimited access between elections.

The team was not limited to these attackers and their direction included direction from the Resolution # 17-05 of the Technical Guidelines Development Committee (hereafter "TGDC") of the U.S. Election Assistance Commission, adopted at the TGDC plenary meeting on January 18 and 19, 2005, which calls for:

". . . testing of voting systems that includes a significant amount of open-ended research for vulnerabilities by an analysis team supplied with complete source code and system documentation and operational voting system hardware. The vulnerabilities sought should not exclude those involving collusion between multiple parties (including vendor insiders) and should not exclude those involving adversaries with significant financial and technical resources."

The Red Team was not trained on best practices for voting systems nor provided general guidelines for the operational, physical, or procedural security practices as practiced by the County and City of Los Angeles, other than that information that was in the technical

data provided by the vendor. Several of the observed vulnerabilities may be ameliorated by such practices (for example, the public observers in the polling place watching the poll workers) but the review and analysis of those practices were out of context for this review.

Operation of the Test

Testing was conducted 2-7 Oct, 2007, in the secure testing facilities in the California Secretary of State's offices. The team consisted of two experts from atsec and a FCMG employee who had participated in the Top to Bottom Review of other systems for California earlier in the year.

Testing began with an introduction and setup by ES&S and ILTS who were to configure the system in a recommended hardened condition for operation and who prepared a test election for use in the testing.

Based on this initial exposure to the system and the industry standard knowledge that errors typically occur at system interfaces, an initial penetration plan was generated which focused on:

- Physical security of the Polling Ballot Counter (PBC) unit of the InkaVote system.
- Physical security of the Ballot Box attached to the PBC at the polling station.
- Contents of the Election Compact Disk created by the Election Generation sub-system of the EMS program.
- Logical security of the files and configuration of the system unit contained within the PBC.
- Logical security of the programs used by and the files generated by the EMS Program, the Election Loader and the Voting Tabulator.
- Security of the networking methodologies used to communicate the election data by the Election Loader to the PBC.

The penetration testing used a combination of manual and automated data collection and analysis methodologies to identify potential areas for exploitation. Testing included but was not necessarily limited to:

- Examination of the top-level system design and architecture (reported under the source code review report);
- Examination of the system documentation and procedures (reported under the source code review report);
- Examination and open-ended testing of relevant software and operating system configuration;
- Examination and open-ended testing of hardware, including examination of unused hardware ports and the security measures to lock/seal hardware ports used;
- Examination and open-ended testing of system communications, including encryption of data, and protocols and procedures for access authorization.

Test tools used included common household and office equipment and chemicals and a number of software Unix utilities, password crackers, and penetration tools readily available over the Internet (specific sources are listed in the confidential report).

Results Summary

Full details will be found in the confidential report. A summary table is found at the end of this report as well as a description of the rating system used. The vulnerability rating assessment is based on the Common Methodology for Information Technology Security Evaluation (CEM v3.1) Rev 1 and Rev 2, App B. The use of this terminology is for convenience in characterizing the potential vulnerability of the system to the identified attack but is not necessarily compliant with and should not be taken as representing a full, formal finding under Common Criteria evaluations.

PBC Physical Access

The PBC System Unit consists of a top half, the PBC head, containing a computer system, ballot scanner, printer, and touch screen display and a connection for the Audio Ballot unit. The bottom half is the ballot box. The election configuration is stored on the computer's hard disk and is used to manage the scanner, printer and the (optionally attached) Audio Ballot unit, to process ballots for the election. A Transfer Device (a USB memory device) may be connected to a USB port housed behind a door on the left side of the side of the PBC that faces the poll worker. The Transfer Device is used to transfer the election data from the PBC to the Election management system (EMS) via the Vote Converter. Although the transfer of results was not included in the limited scope of this study, the port and Transport Device were considered as potential access points in the examination. In transportation of the PBC from storage to the polling place, additional security is provided by a lid that that is screwed down. The user documentation does not specify the use of any tamper proof seals to detect if the lid or PBC have been tampered with during storage and transportation (Ref A.1 in the Summary Table).

In the physical security testing, the wire and tamper proof paper seals were easily removed without damage to the seals using simple household chemicals and tools and could be replaced without detection (Ref item A.1 in the Summary Table). The tamper proof paper seals were designed to show evidence of removal and did so if simply peeled off but simple household solvents could be used to remove the seal unharmed to be replaced later with no evidence that it had been removed. Once the seals are bypassed, simple tools or easy modifications to simple tools could be used to access the computer and its components (Ref A.2 in summary). The key lock for the Transfer Device was unlocked using a common office item without the special 'key' and the seal removed. The USB port may then be used to attach a USB memory device which can be used in as part of other attacks to gain control of the system. The keyboard connector for the Audio Ballot unit was used to attach a standard keyboard which was then used to get access to the operating system (Ref A.10 in Summary) without reopening the computer.

The seal used to secure the PBC head to the ballot box provided some protection but the *InkaVote Plus Manual (UDEL)* provides instructions for installing the seal that, if followed, will allow the seal to be opened without breaking it (Ref A.3 in the Summary Table). However, even if the seals are attached correctly, there was enough play and movement in the housing that it was possible to lift the PBC head unit out of the way and insert or remove ballots (removal was more difficult but possible). [Note that best practices in the polling place which were not considered in the security test include steps that significantly reduce the risk of this attack succeeding but this weakness still needs to be rectified.]

PBS Logical System Access

Attempts to login with invalid passwords without other actions were unsuccessful but the resulting error messages revealed information about the passwords that could be used to reduce the effort for an exhaustive attack of the login passwords (Ref A.5 in Summary).

After the physical box was opened, other methods of gaining access were tried and either succeeded or revealed enough to show that the other attacks were feasible (Ref A.10 in the Summary Table for one such method). Making a change to the BIOS to reconfigure the boot sequence allows the system to be booted up using external memory devices containing a bootable Linux copy (Ref A.11 in the Summary Table). Once done, all the files can be accessed and potentially modified, including sensitive files such as the password file which can be cracked by openly available cracker programs (Ref A.12 in the Summary Table). New users may be added with known passwords and used by the same attacker or other attackers later.

EMS and Election Loader System

The EMS workstations were secured with non-trivial passwords following recommended minimum guidelines. The EMS workstation as installed for the testing were configured with most non-essential services disabled but other potential hardening steps were not used for the test workstations. [The source code review reported errors and other problems with the documentation for the security configuration procedures but the systems tested by the Red Team were configured using hardening practices that were not specified in the technical documentation.] Using standard Microsoft XP features, files were located that held sensitive information which could be processed using publicly available programs. One such file contained the Jurisdiction Key (it was in clear text) (Ref A.7 in summary).

The Election Loader System used an Ethernet connection to install elections to the PBC units. Publicly available software was able to analyze the Ethernet connection which revealed to the Red Team that the connections use standard unencrypted protocols, suggesting that a classic ‘man in the middle’ attack may be feasible (Ref A.13 in Summary). No attempt was made to exploit this attack for this test. [Note: good

operational security procedures should prevent this but the link should still be protected by secure protocols.

Election Distribution CD

The Election Distribution CD, generated by the Election Converter application, is used to pass the election definition to the Election Loader. The Election Loader loads the election to the PBC. Although the CD is described as being encrypted, the Red Team found some files in clear text or partially in clear text which contained critical information. Using the Jurisdiction Key information, the Red team was able to un-obfuscate the Data Encryption Standard (DES) key used to encrypt the Election CD and was then able to decrypt the CD (Ref A.8 in the Summary Table). [The source code team, without the Jurisdiction Key, was able to break down the DES key from information on the CD and create another method for attacking the DES encryption.] Once this key was known, the team was able to breakdown the CD, revise the election definition, and replace the CD with a new encrypted CD with an alternate election definition (Ref A.15 in the Summary Table). The Red Team demonstrated the attack by using the revised to disable the overvote detection feature on the PBC (Ref A.16 in the Summary Table) which is used by LA. The same method could be used to alter vote tallies in the tally function which is not used by LA.

SUMMARY TABLE OF SECURITY TESTING FINDINGS

			Attacker						Vulnerability Assessment					Total
Ref	Title	Component	Voter	Pollworker	Election official	Storage Personnel	Vendor	Scalability	Time	Expertise	Knowledge	Window of Opportunity	Equipment	Attack Resistance
	Red Team													
A.1	Label Security Seals	PBC		X	X	X			0	3	3	4	0	Enhanced
A.2	PBC System Unit Access	PBC		X	X	X	X		0	3	3	4	0	Enhanced
A.3	Seal Procedures	PBC		X		X			0	0	0	1	0	Basic
A.4	Ballot Adding (stuffing ballot box)	PBC	X	X				Low	0	0	3	1	0	Basic
A.5	PBC Linux User/Password Messages	PBC		X	X	X	X		0	3	3	1	0	Basic
A.6	PBC Election/Location Password	PBC		X	X	X	X		0	0	3	1	0	Basic
A.7	Jurisdiction Password	EMS			X	X	X		0	3	3	1	0	Basic
A.8	Election DES Key	Election Converter and Loader			X	X	X		1	6	3	1	0	Enhanced
A.9	Election Distribution CD Cleartext	Election Converter		X	X	X	X		0	0	3	1	0	Basic
A.10	PBC Virtual Terminals	PBC and Audio Booth			X	X	X		0	3	3	4	0	Enhanced
A.11	PBC Access	PBC		X?	X	X	X		1	3	3	4	0	Enhanced

			Attacker						Vulnerability Assessment					Total
Ref	Title	Component	Voter	Pollworker	Election official	Storage Personnel	Vendor	Scalability	Time	Expertise	Knowledge	Window of Opportunity	Equipment	Attack Resistance
	Red Team													
A.12	User Password Cracking	PBC		X	X	X	X		0	3	0	4	4	Enhanced
A.13	Man-in-the-Middle Atttack	Election Converter and PBC			X	X	X		0	6	0	4	0	Enhanced
A.14	Decompile Java Executables	EMS Components		X	X	X	X		1	3	3	4	0	Enhanced
A.15	Fabricate Election CD	Election Loader and PBC			X	X	X	High	1	6	3	4	0	Enhanced
A.16	Disable Overvoting Feature	Election Loader and PBC			X	X	X	High	0	6	3	4	0	Enhanced

Legend for the Summary Table of Security Testing Findings (Red Team):

Vulnerability Assessment Coding:

1. Time to Exploit. "…total amount of time taken by an attacker to identify that a particular potential vulnerability may exist in the [system under test], to develop an attack method and to sustain effort required to mount the attack against the [system under test]. " [CEM v3.1, App B].

2. Expertise. "…the level of generic knowledge of the underlying principles, product type or attack methods " [ibid]

3. Knowledge of Target of Evaluation (TOE). "…specific expertise in relation to the [system under evaluation]" [ibid].

4. Window of Opportunity. "…equate to the number of samples of the [system under test] that the attacker can obtain. This is particularly relevant where attempts to penetrate the [system under test] and undermine the [security features] may result in the destruction of the [system under test] preventing use of that [system under test] sample for further testing, e.g. hardware devices"[ibid]. For this test, the Window of Opportunity includes limitations on accessing a targeted feature.

5. Equipment, hardware/software or other. "…the equipment required to identify or exploit a vulnerability " [ibid]

"Table 3, Calculation of Attack Factor" [ibid]

Factor	Value
Elapsed Time	
≤ one day	0
≤ one week	1
≤ two weeks	2
≤ one month	4
≤ two months	7
≤ three months	10
≤ four months	13
≤ five months	15
≤ six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*[(1)]
Expert	6
Multiple experts	8

Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**[2]
Equipment	
Standard	0
Specialized	4[3]
Bespoke	7
Multiple bespoke	9

[1] When several proficient persons are required to complete the attack path, the resulting level of expertise still remains "proficient" (which leads to a 3 rating).

[2] Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

[3] If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke" "bespoke" is specified when "…clearly different test benches consisting of specialised (sic) equipment are required for distinct steps of an attack"[ibid].

" Table 4, Ratings of vulnerabilities and TOE resistance" [ibid]

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:
0-9	Basic	No rating
10-13	Enhanced-Basic	Basic
14-19	Moderate	Enhanced-Basic
20-24	High	Moderate
≥ 25	Beyond High	

As an example, the PBS Physical Access attack described in A.1 can be done by anyone with access to the PBS (pollworker, election official, storage worker, or vendor) in less than 20 minutes (≤ one day). The attack requires some skill with the locks and seals (Proficient) and knowledge of what the seals protect (Restricted) to be effective. Windows of Opportunity are some what limited (Moderate) because other observers would be expected to respond but the tools were common to home and office use (Standard). The resulting vulnerability to access (total of the factors=10) barely qualifies as Enhanced-Basic which implies that the attack would require more than a casual event.

In contrast, the CD clear text attack (A.8) requires information gained through experience with the system and system documentation (Knowledge of TOE=3) and some common software to review the file contents but does not require additional time (≤ one day) or special tools (Standard). Some knowledge of the system to recognize the files and clear text contents are needed (Restricted). but the clear text may be read by a layman (Layman). The Window of Opportunity requires getting a copy of the CD (Easy). This gives a total vulnerability risk of Basic (Total of factors = 4).

These two examples are both foundation attacks which support other attacks by opening accesses and acquiring Knowledge of TOE that may be used in other attacks.