DEFECTS AND VULNERABILITIES OF THE SMARTMATIC 2010 AES
(or What Smartmatic Must Do To Make Its AES Conformant to RA-9369 In Election 2013)

by
Pablo Manalastas, PhD
IT Consultant, Center for People Empowerment in Governance
Lecturer, Computer Science, Ateneo and U.P.Diliman

The purpose of this paper is to enumerate the errors of the Smartmatic AES that were observed before, on, and after the synchronized national and local elections of May 10, 2010, based on documentation from the Commission on Elections (COMELEC), press reports, and documentary reports of non-governmental organizations like CenPEG.

Our objective is point to technical issues that are apparently clear to IT people, but are not so obvious to ordinary voters. We do not want to destructively criticize Smartmatic. Instead, we want to provide action points that will enable Smartmatic to fix the errors enumerated in this paper, in order to make its AES conformant to the provisions of RA-9369 on automated elections for the Philippines. There is nobility of purpose in this exercise, as it will contribute towards ensuring accurate, secure, auditable computerized elections in 2013 that both the IT community and the Filipino voters can believe in.

Comelec's Interpretation of RA-9369

The COMELEC claims that its interpretation of the provisions of RA-9369 on the following two issues (1) the 60% Filipino ownership of the Smartmatic-TIM joint venture, and (2) making the source code of the selected Smartmatic AES technology available to political parties and interested groups, are the correct interpretations of the law. The Supreme Court even upheld COMELEC's interpretations, by taking the side of COMELEC in the cases Harry-Roque-CCM vs COMELEC, and CenPEG vs COMELEC.

But the correctness of COMELEC's position, and the Supreme Court's imprimatur, leave a bitter taste on the part of the electorate. Despite the claim that TIM owns 60% of the joint venture, we all saw how Smartmatic eased out TIM and assumed 100% control of the execution of the computerized election process. One wonders at this point in time if COMELEC had any participation at all in the exercise, except to say "yes" to all Smartmatic proposals on the computerization details of Election 2010.

Even more bewildering is COMELEC's stand on making the source code of AES 2010 available to political parties and interested groups: (a) First, in May-June 2009, in a minute resolution of COMELEC en banc, it agreed to give the source code to CenPEG, for its own review as provided for by Section 12 of RA-9369. (b) Then in July-August 2009, when COMELEC discovered that Smartmatic did not have a source-code license from original technology owner Dominion Voting Systems, it denied the source code to CenPEG, when CenPEG went to COMELEC's offices to claim a copy the source code. (c) Finally in 2011, after the Supreme Court ordered COMELEC to make available the source code to CenPEG, political parties and interested groups, COMELEC filed a motion for reconsideration, stating that the almost-jail-like-conditions on a source-code-walk-through that COMELEC wanted to impose on the source-code reviewers effectively satisfies the source-code review requirement of Section 12. Any self-respecting IT professional will insist that a code-walk-through under jail-like conditions does not in any way qualify as "own" source code review of the political parties and interested groups.

Thus, these are the environmental conditions under which we propose to enumerate the errors of Smartmatics AES 2010: (a) A COMELEC whose interpretations of RA-9369 could not be accepted

by common sense and by the IT community, (b) A vendor, Smartmatic International, which claims that perceived violations of RA-9369 were put into place because COMELEC ordered Smartmatic to do so. These perceived violations include (b1) the non-implementation of proper CA-issued certificates for digital signing by members of the BEI and BOC, (b2) the disabling of the voter verifiability feature of the PCOS, (b3) disallowing the use of check-marks, cross-marks, and single-dot on the ballot, (b4) disabling the use of the UV-lamp for authenticating valid ballots.

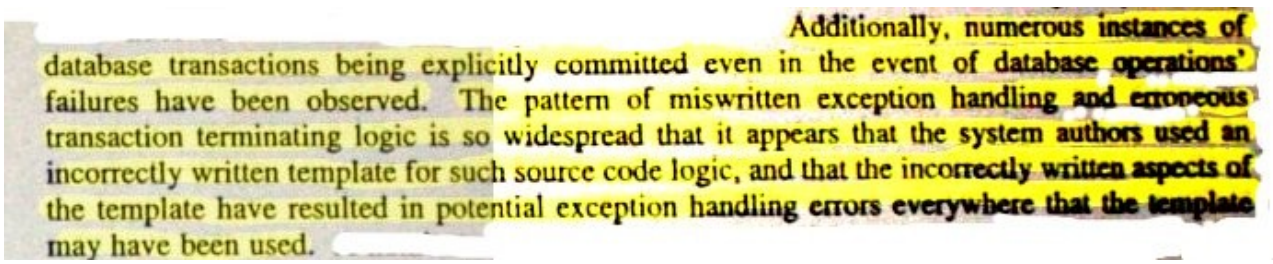
Nevertheless we are constrained to make this listing of Smartmatics' errors, in the face of COMELEC's lack of receptivity, and Smartmatic's hiding under COMELEC's skirt.

Errors Discovered by SysTest Labs

SysTest Labs' source code review[1] found many instances of serious programming errors in Smartmatic's programs that may cause, and actually did cause, execution errors on election day, as evidenced by the PCOS program malfunctioning, the PCOS and CCS allowing transmission of FTS results, and a significant number of tabulation errors in the Comelec's public website.

Also, SysTest Labs did not test the 1,600 election designs produced by the EMS and the EED for each of the 1,600 local municipal/district elections on May 10. 2010, but only tested the artificially contrived data in a hypothetical precinct as supplied by Comelec. Thus there is no way that SysTest Labs could certify that the AES is operating properly, securely, and accurately in accordance with the provisions of RA-9369 because it did not test the AES as it will be used on election day, in the 1,600 local elections.

The most malignant error reported by SysTest Labs concerns database transaction processing, and was described in its report as follows:

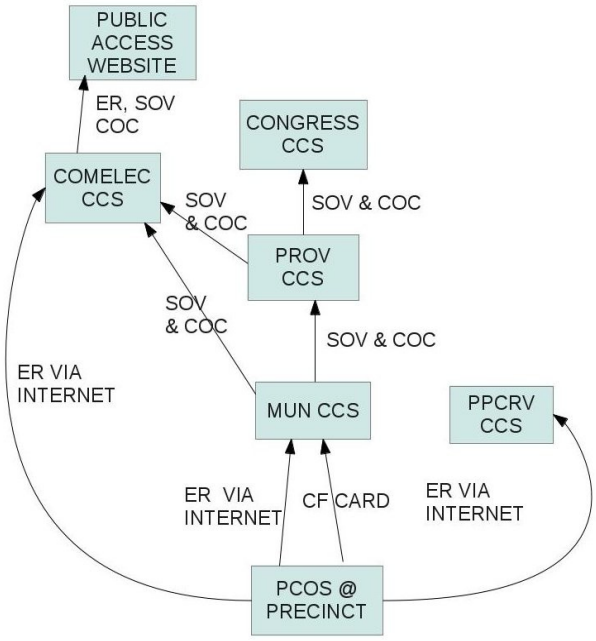

Additionally, numerous instances of database transactions being explicitly committed even in the event of database operations' failures have been observed. The pattern of miswritten exception handling and erroneous transaction terminating logic is so widespread that it appears that the system authors used an incorrectly written template for such source code logic, and that the incorrectly written aspects of the template have resulted in potential exception handling errors everywhere that the template may have been used.

In our experience, such errors in database transaction handling can cause the ballot scanning program, or the vote counting program, or the canvassing program to hang, causing the PCOS or CCS to unexpectedly halt, or to produce the wrong count, or to produce no count at all. Such events as the PCOS computer hanging, or the CCS program producing no count at all, have been religiously documented in CenPEG's report[2] on Election 2010.

PCOS and CCS Transmission Errors

In various COMELEC presentations, we are told that precinct election returns (ER) are transmitted by the PCOS via the Internet to the appropriate municipal CCS, to the PPCRV CCS, and to the COMELEC CCS. If Internet transmission to the municipal CCS fails, the CF card containing the precinct ER is hand-carried by the BEI to the municipal CCS for canvassing. If there is partial failure to transmit, such as failure to transmit one or two candidate positions only, but all other candidate positions are successfully transmitted, then the BEI may not notice the partial failure to transmit, and may actually consider the transmission a success. This partial failure may occur during transmission to the municipal CCS, or to the PPCRV CCS, or to the COMELEC CCS.

The complete transmission diagram is as follows:



In turn the COMELEC (Smartmatic) CCS copies all Internet-transmitted precinct ERs, and all Internet-transmitted municipal and provincial COCs and SOVs to the public access website which was made available for public viewing at the link, http://electionresults.comelec.gov.ph, on May 10, 2010, and several weeks thereafter. We made a mirror of this website, so that several months after COMELEC took the original website down, we have made a mirror website available at http://curry.ateneo.net/~ambo/ph2010/electionresults/index2.html.

A study of the COMELEC public access website[3] reveals evidence of large scale transmission errors. Of the total of 76,472 precinct ERs, we have counted (using computer programs to count) the following:

Precincts that have no ERs, possibly due to transmission failure	8,939	11.7%
Precincts that have too few voters (0-10), possibly FTS ERs	371	0.5%
Precincts that have normal (> 10) number of voters	67,162	87.8%
Total number of precinct ERs counted	76,472	100.0%

The disturbing fact is that of the 67,162 precincts with normal number of voters 25,888 precincts or 38.5% have missing data in one or more candidate positions.

The web page of a precinct with no ER, possibly due to complete transmission failure, looks like this:

A precinct that has too few voters (0-10), possibly because the FTS result was already accepted by the CCS, before the actual election day ER, looks like this:

COMMISSION ON ELECTIONS
REPUBLIC OF THE PHILIPPINES

Philippines 2010 Elections Results »

Results Date: May 22, 2010 2:45:08 AM PHT

The Philippines > II > ISABELA > ANGADANAN > CP 27 0066A, 0067A, 0068A, 0068B

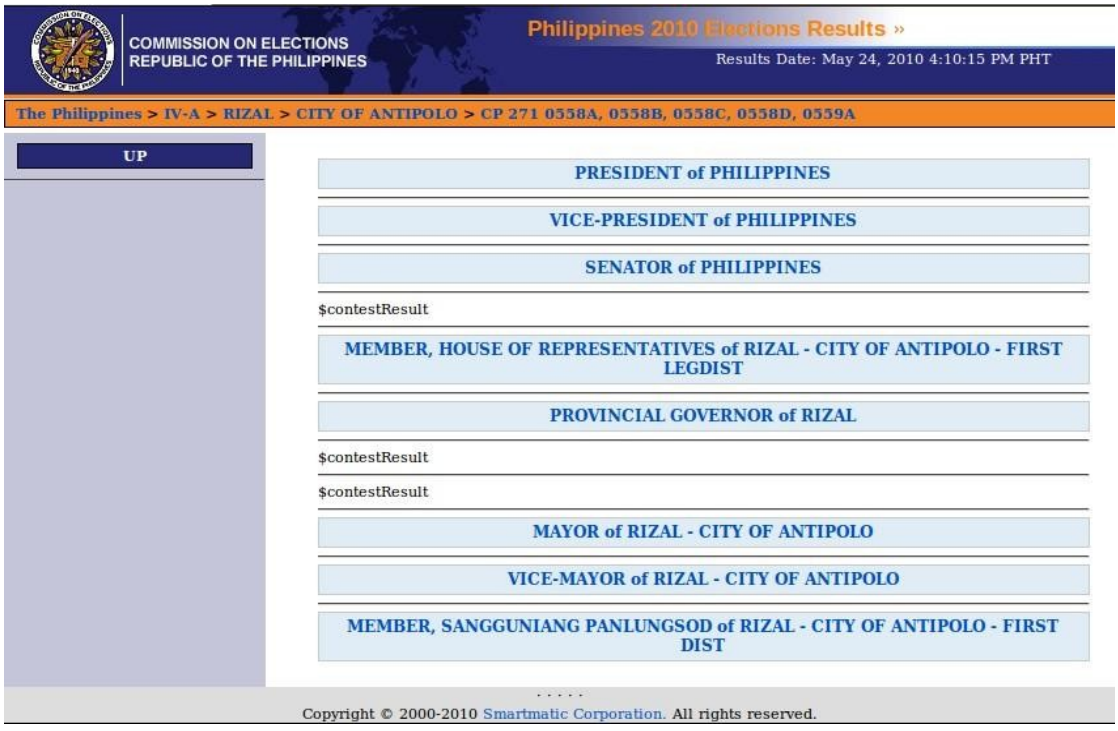
UP

PRESIDENT of PHILIPPINES

Candidate	Party	Votes	Percentage
VILLAR, Manuel Jr B.	NACIONALISTA PARTY	4	40.00%
ESTRADA EJERCITO, Joseph M.	PWERSA NG MASANG PILIPINO	3	30.00%
AQUINO, Benigno Simeon III C.	LIBERAL PARTY	2	20.00%
VILLANUEVA, Eduardo C.	BANGON PILIPINAS	1	10.00%
DE LOS REYES, John Carlos G.	ANG KAPATIRAN PARTY	0	0.00%
GORDON, Richard J.	BAGUMBAYAN-VNP	0	0.00%
ACOSTA, Vetellano S.	KILUSANG BAGONG LIPUNAN	0	0.00%
PERLAS, Jesus Nicanor P.	INDEPENDENT	0	0.00%
TEODORO, Gilberto Jr. C.	LAKAS KABALIKAT NG MALAYANG PILIPINO CHRISTIAN MUSLIM DEMOCRATS	0	0.00%
MADRIGAL, Jamby A.	INDEPENDENT	0	0.00%

Statistics	
Total number of Voters who actually voted	10

A normal ER, but with no data in one, two, or three candidate positions, possibly because of partial failure of transmission, looks like this:



COMMISSION ON ELECTIONS
REPUBLIC OF THE PHILIPPINES

Philippines 2010 Elections Results »

Results Date: May 24, 2010 4:10:15 PM PHT

The Philippines > IV-A > RIZAL > CITY OF ANTIPOLO > CP 271 0558A, 0558B, 0558C, 0558D, 0559A

UP

PRESIDENT of PHILIPPINES

VICE-PRESIDENT of PHILIPPINES

SENATOR of PHILIPPINES

$contestResult

MEMBER, HOUSE OF REPRESENTATIVES of RIZAL - CITY OF ANTIPOLO - FIRST LEGDIST

PROVINCIAL GOVERNOR of RIZAL

$contestResult

$contestResult

MAYOR of RIZAL - CITY OF ANTIPOLO

VICE-MAYOR of RIZAL - CITY OF ANTIPOLO

MEMBER, SANGGUNIANG PANLUNGSOD of RIZAL - CITY OF ANTIPOLO - FIRST DIST

We asked COMELEC (on two occasions) to check if these precinct ERs in the public access website with missing data in a few candidate positions, have corresponding precinct ERs in the municipal CCS, but with no missing data at those candidate positions. So far COMELEC has not yet given us an answer. If these two versions of the ER are exactly the same, then not all the votes

in those 25,888 precincts have been canvassed and consolidated – in this case about 12.9 million voters have been partly disenfranchised because their votes for one, two, or three of their candidates were not included in the canvassing.

Monday, March 12, 2012

References

[1] SysTest Labs , “Certification Test Report for Source Code Review, Readiness and Security Testing: Philippine AES Voting System”, February 9, 2010

[2] http://www.cenpeg.org/The%20CenPEG%20Report/The_CenPEG_Report.html

[3] http://electionresults.comelec.gov.ph/ or http://ibanangayon.ph/