TRANSPARENCY AND INFORMATION SECURITY IN AN AUTOMATED ELECTION SYSTEM

Transparency and information security… two concepts that appear to be poles apart.

Transparency espouses openness. Information security, on the other hand, is secretive in the manner of its implementation.

Batas Pambansa No. 881 or the Ominibus Election Code is a guide on how transparent our elections are by providing detailed procedures in voting, counting, and consolidation of votes.

Republic Act No. 9369 entitled "An Act Amending Republic Act No. 8436, Entitled "An Act Authorizing the Commission on Elections to Use an Automated Election System in the May 11, 1998 National or Local Elections and in Subsequent National and Local Electoral Exercises, to Encourage Transparency, Credibility, Fairness and Accuracy of Elections, Amending for the Purpose Batas Pambansa Blg. 881, as Amended, Republic Act No. 7166 and Other Related Elections Laws, Providing Funds Therefor and for Other Purposes," requires that the automated election system operate securely, accurately, and properly.

This paper examines how these concepts find their place in an automated election system.

TRANSPARENCY AND INFORMATION SECURITY IN AN AUTOMATED ELECTION SYSTEM

By: **ANGEL S. AVERIA, JR.**
President, PHCERT
IT Consultant, EU-CenPEG Project 3030
June 8, 2011

INTRODUCTION –

We have been witnesses to the conduct of manual elections in the country. Tainted with cheating in varying degrees, vote manipulation and vote padding and shaving (*dagdag – bawas* or vote-padding and -shaving), automating the Philippine elections was seen as a solution to this problem. 2010 saw the implementation and use of an automated election system on a nationwide scale. There were differences of opinion on how the system operated. In the run up to the elections, a major problem caused fear and anxiety among the stakeholders. In the election aftermath, complaints of fraud filled the air. On election day and days following, a number of problems were noted, observed, identified, and documented.

The Automated Election System as Implemented –

Let us first examine how the automated election system was implemented by the country's election manager:

- Voting and counting machine at the precinct level which allows the voter to cast his vote using a paper ballot and at the end of polling counts the vote. This same machine transmits the election returns to the city/municipal canvassing machine.

- The canvassing machines at city/municipal, provincial, and national levels. The canvassing machine at city/municipal level receives the election returns from the voting and counting machines stationed within its jurisdiction and consolidates the vote counts. The provincial canvassing machines receive the certificates of canvass and supporting statement of votes from the city/municipal

canvassing machines within the respective provincial jurisdiction and consolidates the votes. The national canvassing machine receives the electronic certificates of canvass and supporting statement of votes from the various provinces and consolidates the votes.

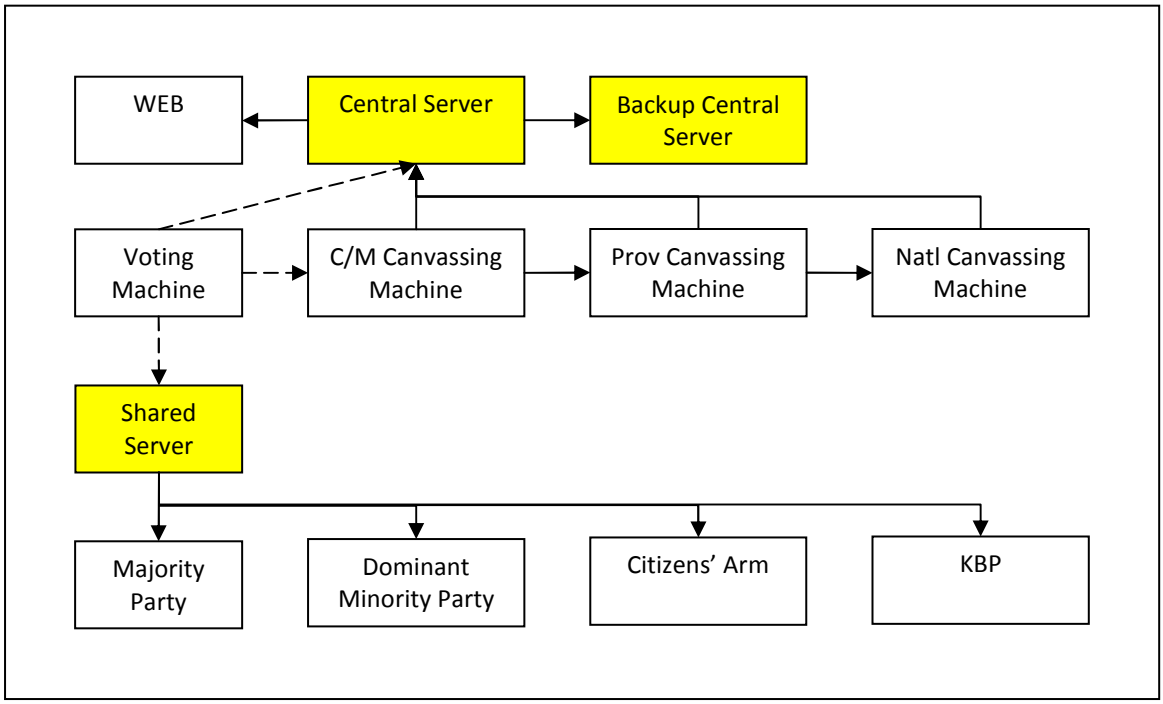
- A website where the election returns are also supposed to be posted.

- Linking the voting and counting machines and canvassing machines is the telecommunications infrastructure.

- In addition, electronic election returns are transmitted to a shared server which relays the election returns to the machines of the majority party, dominant minority party, accredited citizens' arm, and the Kapisanan ng mga Brodkaster ng Pilipinas.

- The election results and election reports were also transmitted to a central server (and its backup) operated by Comelec.

A simple diagram* represents the whole network as implemented in the last NLE:



* Based on observation and publicly available information. The Comelec and Smartmatic-TIM did not disclose the network topology for reasons of security.

TRANSPARENCY –

The International Foundation for Electoral Systems defines transparency, thus:

> "Transparency is the term for clear and open process, which is understandable and accountable to the electorate. Transparent procedures encourage participation in and support of the electoral system.
>
> "Transparency is essential to the electoral process because it eliminates the appearance of impropriety and limits the possibility of electoral fraud. Transparent procedures promote public confidence and trust in the electoral system."
>
> A Guide to Transparency in Election Administration
> By: Constance Andrew Kaplan, IFES Consultant

Batas Pambansa No. 881 or the Ominibus Election Code is a guide on how transparency is ensured in our elections by providing detailed procedures in voting, counting, and consolidation of votes. For the counting of votes, the law provides that the ballot being examined for counting must be in full view of observers. The law specifies how the room where the counting of votes is to be done will be arranged – the position to be taken by the members of the Board of Election Inspectors, the position of the observers relative to the position of the Board of Election Inspectors, the location of the tabulation sheet, etc. The law provides rules or guidelines on how the ballot is appreciated. Similarly, the law describes how the canvassing and consolidation center is to be arranged, allowing full view of the election reports by observers of the canvassing and consolidation of votes. BP881 law also provides the procedures for the receipt of election returns, how the election returns are to be examined and authenticated, and how the results documented in the election returns are to be recorded in the

statement of votes and the certificate of canvass. The process of ballot appreciation, recording of votes, and counting of votes and the process of canvassing and consolidation at various levels were guaranteed by BP881 to be open and observable by the public.

Transparency in the Automated Election System –

The same level of transparency as defined by BP881 was not evident in the automated election system used in the elections of May 10, 2010. Observers did not see how the machine recognized the vote selections, how the votes were credited to selected candidates, how the votes were counted, and how the votes were consolidated at various levels. However, as a small measure of transparency, RA9369 required that the election returns generated by the voting machine be printed and posted on the door of the precinct for a defined period and copies of the same distributed to pre-determined parties and groups. The law also requires that the election returns be posted in a publicly accessible website from which interested parties may be able to download the election returns for their own consolidation. RA9369 also requires that the certificates of canvass be printed out, posted on publicly accessible location in the canvassing center, and copies distributed to pre-determined parties and groups.

An automated system is never transparent as the execution of automated processes is not observable. To make the automated processes observable, the programmed commands must be executed in a step-by-step manner with the results at each step displayed to observers. This effectively negates one of the goals of automation – speed. By doing this slow process in an automated election system, the process of recognizing and crediting of votes, for example, will probably take longer than the manual process.

Technology Solutions for Transparency –

Technology solutions offer limited transparency to the automated electoral process, such as the printing and posting of election results and the distribution of copies of the election results to pre-determined parties

which RA9369 already requires. LCD projectors may be used to display the election reports at canvassing centers.

Disclosure as an Alternative –

How can transparency in an automated election system be implemented?

RA9369, in requiring the publication of results as a transparency measure, also required public disclosure (though the law did not use this term) by mandating that the following be done:

- Source code of the automated election system be reviewed by interested political parties and groups,
- Public testing of the system and examination of results
- Conduct of a random manual audit

Each of these activities may be done using scientific methods by information and communications technology professionals and practitioners with experience and expertise. *(Papers discussing the need for source code review and the conduct of random manual audit will be presented separately.)*

Does disclosure sufficiently meet the standards of openness and transparency? This paper posits that it does. The findings in the conduct of the source code review, public testing and examination of results, and random manual audit may be published for the public to review. For wider participation, publication may be done via the internet. Stakeholders, especially those with knowledge and expertise in application development, system quality assurance, and audit practice, will be able to contribute ideas on how to improve the system and propose solutions to problems or deficiencies of the system, if any is found and disclosed. Disclosure will encourage those interested to participate in improving the automated election system and is seen to generate public confidence and trust in the automated election system.

SECURING THE AUTOMATED ELECTION SYSTEM –

Automating Philippine Elections was seen as a cure to cheating. Therefore, a need to make sure that the automated election system is secure and protected from unauthorized access. RA9369 requires that the Technical Evaluation Committee certify that the automated election system is operating properly, **securely**, and accurately.

Information Security –

Information security practitioners and professionals are quite aware that information security rests on the concepts of confidentiality, integrity, and availability. A failure in the implementation of one concept spells a failure of the whole information security net. There are many available technology solutions that may be implemented to ensure that confidentiality, integrity, and availability are ensured.

Information security seeks to protect not only the data stored, processed, and transmitted and received in an automated system but seeks to protect the whole physical infrastructure, including the telecommunications infrastructure, each machine connected to the network, and all network components.

It is easy to see from the diagram presented above what we seek to protect:

- Each component in the whole infrastructure
- The data transmission infrastructure, wired or wireless
- Data:
    - ballot, vote record, vote count, election return stored in the voting and counting machine
    - election returns as received by the city/municipal canvassing machines
    - certificates of canvass and statement of votes in each canvassing machine at all levels of canvass

Confidentiality –

The need for confidentiality, that is, the need to protect the secrecy of the ballot, in an automated election system is more pronounced at the voting stage. Apart from the manual exercise of protecting the ballot as this is being filled out from prying eyes, the processes implemented in an automated election system must ensure that vote is not traceable or identifiable to any voter. For instance, in the last elections, the ballot used in the May 10, 2010 elections is marked with a bar code. Embedded within the barcode are the province code, the city or municipality code, and precinct code all of which identify the ballot with a specific precinct where the ballot it is to be used. But unknown to many, the bar code also includes a serial number. This was revealed by representatives of Comelec in a forum held about 20 months before the elections. On the one hand, the serial number ensures the uniqueness of the ballot. But the serial number could allow anybody creative enough to set up a simple system that will be able to match each ballot with the identity of the voter to whom the ballot is issued.

Technology Solutions to Ensure Confidentiality –

To ensure confidentiality of the ballot, solutions must be devised that will ensure the uniqueness of a ballot, paper-based or electronic, but at the same time prevent traceability. For instance, random numbers may be used instead of serial numbers. To further ensure non-traceability, the ballot and the corresponding vote record (a record of how the machine appreciated the ballot) may be written randomly in data storage devices.

To ensure that only genuine ballots (in the case of paper ballots) are received by the voting machine, machine detectable security features must be embedded on the paper ballot.

Integrity –

A set of guidelines (as provided in BP881) is used to appreciate a ballot in a manual system. The same must be true for an automated election system. An automated voting machine must be so designed following a set of vote appreciation rules so that the machine appreciates a ballot reflecting the true intent of the voter.

The information processed must remain the same all through out in the system.

The election results must be generated accurately and must be protected from unwarranted manipulation while in the storage and during transmission to preserve integrity in every stage of the automated election system.

To assure the voter that the vote record generated by the voting machine reflects his true intent, the voter verifiability feature as required by RA9369 must be properly implemented.

Technology Solutions to Ensure Integrity –

- Digital signatures on the election reports. RA9369 requires that the election reports be digitally signed. Digital signing must be properly implemented. Each member of the Board of Election Inspectors (BEI) and Board of Canvassers (BOC) must each have their personal digital signature. The would be members of the BEIs and BOCs must be properly trained on the technology of digital signatures to the extent that they are to be personally and individually acquired, not assigned.
    - Acquiring digital signatures is a stringent process. Since the members of the BEIs are usually public school teachers and members of the BOCs are usually Comelec employees or city/municipal officials or employees, a web of trust may be developed. Such web of trust will reflect the hierarchy of the Department of Education, the Comelec, and the city/municipality.
- Hash Code. As a second layer of data protection, ballot images (in the case of paper ballots) may be captured and a hash code generated for each ballot image. Similarly, the hash code of each vote record and election report may also be generated.
- Encryption/decryption. As a third layer of protection, election reports may be encrypted prior to transmission and decrypted on receipt.

- Transmission channels must be protected using appropriate technologies, such as VPN tunneling and using SSL and similar such data protection protocol.
    - Confirmation of receipt must be sent by the receiving machine to the sending machine.
    - A receiving machine will receive election reports only from sending machines within its jurisdiction.

To protect the individual hash codes, said hash codes may be kept in a file (in a voting or canvassing machine) and a hash code of the file also generated and the file itself protected from tampering by having that file digitally signed and, if necessary encrypted.

Availability –

Software and hardware availability must be ensured.

To ensure software availability, the software must undergo appropriate tests, including stress tests, prior to deployment.

At the physical level, all hardware components must similarly be thoroughly tested.

To ensure availability of the whole infrastructure, redundancies must be considered when the network is being designed. The network must be fully tested before it is put into operation.

To further ensure availability of the system, a continuity plan or disaster recovery plan must be put in place. Replacement components and/or parts must be provided in strategic locations, always at the ready for deployment.

Where such replacements cannot be made available, alternative actions must be considered.

In the event of transmission failure or non-availability of transmission facilities, alternative actions may be defined such as the hand delivery of storage devices to the canvassing center. In this event, the software must

be so designed such that it will identify which report was received via transmission facilities and which ones are directly uploaded from a storage device.

Data Consistency –

To maintain consistency in the database, as the central server receives all transmissions, those reports uploaded from storage devices must be transmitted to the central server by the canvassing machine used to upload such reports. Uploaded reports must be properly tagged, identifying specifically the source of the report.

No election reports must be received by the canvassing machines and central servers dated prior to election day.

Identity Management –

Users and operators form part of the information security puzzle.

- The voter who will have access to the voting and counting machine at the time he casts his vote
- The members of the Board of Election Inspectors who shall operate the voting and counting before the opening of polls and after closing of polls
    - The technical support staff who will assist the Board of Election Inspectors in the event of problems with the voting machine
- The members of the Board of Canvassers at all levels of canvassing who will operate the canvassing machines
    - The technical support staff who will assist the Board of Canvassers in the event of problems with the canvassing machines
- Operators of the central and backup data centers, including website operators for posting of election reports.
- Operators of each recipient parties – majority party, dominant minority party, accredited citizens' arm, and KBP.

- Others who will be given access to the system for purposes of repair, maintenance and support and for other purposes.

All of these users must be given the appropriate access authorities specific components of the automated election system.

Access mechanisms must also be installed in data centers where central and backup servers may be installed and operated.

Audit Logs –

Activity logs must be embedded in each system component – the voting machines, canvassing machines, servers, workstations and other access devices. All activities triggered by human intervention or those processes executed by the automated election system components are recorded.

Hardware Protection –

The hardware must be so designed in manner that prevents or limits connectivity. Only the necessary communication or access ports must be made available. For instance, an external modem will require a modem port. It would be more desirable to have the modem integrated in the hardware so that no modem port will be made available externally. If such ports are made available, it is best that such ports are set by default to disabled and may be enabled only at the time of need, enabling the same by software function.

Security by Design –

At the onset, design of the automated election system, both hardware and software, must address the security considerations. Threat analysis is a good strategic approach to hardware and software design and development. A careful study and review of the hardware and software platforms must be done and vulnerabilities reviewed. Vendors of hardware and software issue vulnerability bulletins and the appropriate patches. Programming language nuances must also be taken into consideration. Is "=" the same as "=="? The alphanumeric character ";" when provided in an

entry field allows access into an SQL database and this has been used by hackers to exploit the database. Such nuances, if not addressed at the program development stage become the security holes that will enable ill-intentioned parties to exploit the system.

TRANSPARENCY AND INFORMATION SECURITY –

Transparency and information security may appear to be strange bedfellows. But both concepts can co-exist. Demonstrating how a security solution works is part of disclosure. For example, showing how digital signing can protect an electronic election return from tampering will allow the public to understand the technology and appreciate the protective measures that are implemented in the system. Disclosing the language to be used and inviting public comment may lead to exposing language nuances and vulnerabilities which may help developers to properly address such nuances.