Hybrid Cryptography for

Automated Election System

Hipolito, Jovellano, Pachico

Abstract

The Philippines has been adopting the Automated Election System after years of adhering and relying on the Manual Voting System. It has been proven that the process became more efficient and generates results in a lesser time frame. However, complications are still evident in present time. For instance, the possibility of electoral fraud still continues to persist through the existence of a secret server in the last presidential election. This study aims to propose a technical solution that would eliminate the possibility of secret servers by implementing a public key infrastructure as security measures for the transmission of votes on the server-level.

INTRODUCTION

Background of the Problem

After years of having a manual voting system, the Philippines have finally adopted an Automated Election System (AES) in 2010. This was mandated by Republic Act No. 9369 which is the Amended Elections Automated Law. The law stated that there would be paper-based election system defined as “a type of automated election system that uses paper ballots, records, and counts votes, tabulates, consolidates, canvases, and transmits electronically the results of the vote counts.” (Angkaya, 2011).

By standards, the new technology should be significantly more accurate and reliable for the voters; however, there were still some problems that might prove the acquired AES otherwise. For instance, the current automated election system with SMARTMATIC uses compact flash (CF) cards for the configuration of the Precinct Count Optical Scan machines in different provinces. These CF cards are pre-loaded with the precinct’s ballot depending on its specific geographical data. Then the same CF cards will also be the ones to store the data of the votes of the people. To look at it clearly, the cards are pre-loaded and will also be the storage of the votes and elections results. Now, this situation gives candidates, who want to sabotage the election, an easy time to manipulate the data in the system because it can definitely be intercepted through physically tampering with these so-called CF cards. The study aims to find a way to reduce electoral fraud in the counting and transmission part of the automated election system in order to achieve an indeed accurate and reliable system.

The Automated Election Systems in the Philippines follows a sequence of process. Focusing on the counting and transmission module of the system, the process starts when the polling precincts closes on the election day. The PCOS machines transmit the vote counts or election returns to the corresponding servers and canvassing centers. It is done chronologically with a hierarchical structure composed of the precinct level, municipal level, provincial level, regional level, and national level. From the PCOS machines, the ERs are transmitted to the central server, to a transparency server, and to the municipal board of canvassers (MBOC). From the MBOC, the results are brought to the provincial board of canvassers (PBOC) or the regional board of canvassers (RBOC), where the results are collected and then transmitted to the national board of canvassers (NBOC), where the results for national positions are canvassed. The MBOC and PBOC also separately send ERs to the central server. Moreover, the canvassing system processes the ERs that were transmitted. Public telecommunication networks are assigned to be the main channel when transmitting the ERs. There are back-up plans made if the network fails to accomplish its task. For example, transmissions can be made via satellite to avoid delays when problems occur.

During the course of the counting and transmission of ERs, electoral fraud is inevitable. There are a lot of issues concerning the effectivity and efficiency of the machine during the elections. For instance, the current voting system does not incorporate digital signature when transmitting the election returns from precincts to canvassers even if it is stated in the law. According to the republic act 9369 section 22, *“The election returns transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate”.* This means that BEIs are required to digitally sign the ERs that would be transmitted. As stated in the law, the ERs that would be recognized officially are the ones that were authenticated and validated by the administrators. However, during the past three automated election system, the AES failed to meet the requirements prescribed by the law. A possible reason is that the system being used allows humans to intervene in the process of the election. This is one of the reasons why it is easy for any unofficial institutions/organizations to ambush and manipulate the elections. For example, in Mindanao armed men prevented the citizens from voting. They controlled the precinct and made it impossible for the voters to cast their votes. Many eye witnesses claim that a wholesale ballot shading was conducted. Meaning only the same people casted many ballots inside the PCOS machine without the control of the BEIs. Without the existence of a digital signature provided by an authenticated agency, the election returns being transferred would still be considered not reliable because the digital signatures are used to verify the validity of the transmitted ERs. A public key infrastructure is practiced to guarantee that the votes are secured during transmission. A system should be designed to ensure that before transmitting the votes, ERs are equipped with digital signatures. Another solution that could be made to reduce the chances of this type of cheating is to incorporate the idea of GPS or global positional system in the machine used in the elections. GPS tracking uses both the time and location components that could provide data to the users. It is an effective way of navigating where the machine should be placed or located via a system the receives data from the satellites in space.

Statement of the Problem

How can the Philippine automated election system eliminate the possibility of secret servers to secure the transmission of election returns on the server-level?

Objectives

General

* To know the vital issues currently present in the transmission of the votes
* To propose a system that would prevent electoral fraud in the transmission of votes in the automated election system

Specific

* To provide a technical solution that allows the verification of the servers’ authenticity through the use of a public key infrastructure as a security mechanism

Significance of the Study

The findings of this research will benefit the following key players:

To the Filipino Citizens

This study will benefit the Filipino citizens for ensuring the security of the casted votes. Also, it would prevent malicious individuals from manipulating the votes. Although the nature of automation easily provoke fear to ignorance of using technology, this study will educate some of those users that still lack computer literacy foundation. Indeed, education can bridge the existing gaps and even remove the unnecessary fear from automation. This will leave the citizens better equipped for the future of the Philippine automated election system.

To the COMELEC

This research would significantly contribute to the goal of the COMELEC to conduct a fair and transparent election. Considering the impact of the elections in the overall condition and future of the Philippines, it is important to make sure that the voters’ choice reflect the outcome of the election. To do that, the system should be able to prevent and mitigate electoral fraud while ensuring that the voters have casted their votes in a way that is convenient and voter-friendly. This study will aim to determine the most appropriate methods to achieve the kind of system that does not manipulate the vote of the people in any way through data gathering and research. In this manner, the people will be knowledgeable about how the system works and be informed and wise voters themselves.

To the Future Researchers

As the Philippines adjust to this kind of voting system, more and more developers would also contribute to the AES aspect of software development. In that case, the system that would be created can serve as a guide and inspiration for other developers who would want to pursue the prospect of automated election system too.

Scope and Limitation

The scope of the study would only include the issues and possible solutions for the security of the transmission of election returns on the server-level of the automated election system in the Philippines. Further study on the other parts of the automated election system will no longer be covered.

REVIEW OF RELATED LITERATURE

Related Literature

**How does the current automated election system work?**

On election day, as the polls close, the BEI immediately administers the transmission of the votes or election returns via the PCOS machines equipped with modems to the servers and canvassing centers The Electronic Results Transmission Service is responsible for the transmission of the votes. The primary channel used is through the public telecommunications networks and if that fails transmission will then be run through the satellite. Furthermore, a software called the Real-time Election Information System, reads the data and canvasses the votes. After the transmission from the PCOS machine, the ERs are transmitted to the central server, to a transparency server, and to the municipal board of canvassers (MBOC). Those three are the official servers declared by the administrators or officials of the elections. Moreover, the MBOC transmits it to the provincial board of canvassers (PBOC) where they consolidate and later transmit the results to the national board of canvassers (NBOC). Additionally, both the MBOC and PBOC sends ERs to the central servers.

There was a special case in ARMM wherein they establish the regional board of canvassers (RBOC). The results for ARMM governor, vice governor, and assemblymen are tallied before being transmitted to the central server.

During the 2016 elections, congress will have their own server wherein the members of the senate and house of representatives can monitor the canvassing of the votes and to officially proclaim the winner for the national level. (Retrieved on August 27, 2016 / <http://www.rappler.com/newsbreak/iq/91663-philippine-automated-election-sytem-explained>).

**How can electoral fraud occur in the system?**

Lack of Digital Signature

Digital Signatures serve two purposes during the elections. First, to ensure that the precinct election returns are not changed or modified throughout the election period. Also, this can help identify the BEI personnel in charge of the election returns as well as the precinct number it came from. However, based on a report by the Carter Center, the emphasized the absence of a personnel in charge of generating the public and private keys that should be used in the digital signatures as part of the transmission module for election returns in the automated election system. They had agreed that given the situation it has been one of the basic and fundamental system flaw that they’ve encountered. Apparently, the people administering the election abandoned the idea of implementing the digital signatures thus gaining a larger chance of having fraud during the elections. As prescribed in the RA 9369 Section 19 A, the digital signature is a vital part in maintaining the integrity and security of the election returns being transmitted. The law states that, “The election returns transmitted electronically and digitally signed shall be considered as official election results…”. With this, it can be inferred that the people behind the automated election system are not meeting the requirements needed thus violating the law. Also, the results of the election generated by the automated election system is now being questioned with regard to its integrity. The automated election system’s ability to bring and conduct an election in the most effective and efficient way is currently being doubted by a mass of people. (Retrieved on August 15, 2016/ <http://romeocayabyab.com/controversial-2010-philippine-automated-elections-revisited/>).

Secret Servers

During the 2016 elections, Bong Bong Marcos’ camp believes that there exists a “Fourth Server” or also known as the “Queue Server”. It has been revealed that the Comelec and Smartmatic has been keeping it from the public. Instead of letting the ERs be directly transmitted to the three official servers, namely the Municipal Board of Canvassing Server, Comelec Server, and the Transparency server, the results were first being processed and consolidated in the “Queue Server”. Another problem with the secret server is that the source code being used was never reviewed despite of it being a requirement in the law. Moreover, there were no poll watchers assigned for these servers making it questionable to both the public and the administrators. According to a statement made by Rodriguez, a representative of Marcos’ camp, the integrity of the 2016 May elections has been questioned because of the unexpected situation made by the Comelec and Smartmatic. The ERs that were presented to the public did not come directly from the transparency server. Alternatively, the results were first transmitted to a “Queue Server” where they were “consolidated and processed” and the “Queue Server” sends the data to the transparency servers which is against the law. (Retrieved on August 10, 2016/ <http://www.manilatimes.net/smartmatic-admits-using-unofficial-servers/275442/>).

**How can the automated election system be secured specifically for the counting and transmission?**

The Philippine Government in collaboration with the Department of Information and Communication Technology and Department of Science and Technology established an Integrated Government Philippines Project. It seeks to lower the cost of government information and communication technologies (ICT) by using cloud computing services. The project aims to increase productivity, to develop excellent services, and at the same time to reduce the value spent on this development. The agencies that would first be targeted by this project are the National Government Agencies and Government-Owned and Controlled-Corporations (GOCCs), including State Universities and Colleges (SUCs). (Retrieved on August 10, 2016/ <http://i.gov.ph/philippines-cloud-first-policy-draft-4/>).

Following the controversial secret server, the Commission on Elections is one of the three constitutional commissions of the Philippines which means that they can utilize this project to have a more effective approach with regard to the automated election system. By doing so, there is a chance that electoral fraud committed during the counting and transmission of the ERs would be lessen. The said project is already being developed to provide high-speed communication and to increase the security of the data being kept. This is design to prevent hackers from attacking or penetrating government-related information in the cloud. It also promotes transparency which is also a requirement during the local and national elections. The project being conducted can be one of the possible solutions that can be done to prevent electoral fraud in the counting and transmission module of the automated election system. (Retrieved on August 10, 2016/ <http://i.gov.ph/philippines-cloud-first-policy-draft-4/>).

The Integrated Government Philippines or iGovPhil project and the E-government Master Plan that aims to provide National Government Agencies and Government-Owned and Controlled-Corporations (GOCCs) cloud computing services. In order to achieve their desire, a Public Key Infrastructure will be applied in the said project. It will ensure that the service provided can meet the objectives of ensuring the security and reliability of all transactions online. Also, the PKI is an important component of the project by DOTC and DICT. The role of the PKI is to let the users or consumers of public networks to securely transfer data. An important aspect in the PKI is its capability of creating, distributing, storing, using and revoking digital certificates. The certificates are small files that secures the integrity of the data and at the same time verify or authenticate that the sender of the data is the source. This will prove that the data being transferred has not been tampered. Additionally, the infrastructure can be utilized to encrypt data.

There are a number of reasons as to why using PKI is more efficient and effective in securing data exchange. One of which is that it improves an individual’s identity verification process. The Digital Certificate distributed by the PKI will have a minimum 2048-bit system generated key which is better compare to the usual 80-bit security being implemented in passwords. The 2048-bit system security will ensure that the individual’s identity is verified. It lowers the inconvenient ways that a user must possess in order to prevent data breaching made by perpetrators. Moreover, other countries including the Philippines are bounded by law which states that only digitally signed data are to be recognized or accepted as evidence in the court of law. This makes the document tamperproof because one small change which can be equivalent to 1-bit will be under suspicion and be detected during the verification process. Additionally, the PKI protects data from intruders trying to enter the system. As years passed, people are leaning on the side of ICT and its future developments. However, methods of encryption are being refined to ensure the integrity of the system. Data encryption is used to further enhance the level of security of each system and currently there are a number of algorithms that can be used depending on the level of confidentiality each data has. (Retrieved on August 19, 2016 / <http://i.gov.ph/pnpki/> ).

Related Study

Experimental Design of Worldwide Internet Voting System using PKI

In this study, the researchers designed an Internet voting system applicable for worldwide voting which was based on Ohkubo et al.’s scheme combined with Public Key Infrastructure. In the system, voter’s privacy was guaranteed by using blind signature and mix-net, and robustness which was provided through the threshold encryption scheme. A way of typical implementation for internet voting system was proposed by employing Java technology. PKI allowed worldwide key distribution and “one certificate/one vote” policy. Therefore, anyone can participate as long as a certificate was given by Certificate Authority (CA). By the joint work between Korean and Japanese teams of this study, the implementation aimed to select MVPs in 2002 FIFA World Cup Korean-Japan in easy and friendly manner for any internet user to participate. (Retrieved on August 27, 2016 / <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=311B92E00249A90FA1A9557F7E3ABA46?doi=10.1.1.6.1111&rep=rep1&type=pdf>). In this study, it was showed it is possible to incorporate a PKI in a voting system. Not only it was possible, it was also recommended for security purposes of the system.

THEORETICAL BACKGROUND

A Public Key Infrastructure is a combination of software and procedures providing a means for managing keys and certificates and using them efficiently. Key and certificate management is the set of operations requires to create and maintain keys and certificates. One of the major points being addressed in a managed PKI is the creation of keys and certificates. A PKI must offer software support for key pair generation as well as certificate requests. Furthermore, there must be procedures to verify the identity of the user before allowing him to request a certificate. Next major point is private-key protection. These private keys are either used for decryption or digital signature so it has to have some reasonable level of protection. In this case, a strong password mechanism must be implemented to have an effective PKI. Now, if the user’s private-key has been compromised, the PKI must provide a means by which a certificate can be revoked. Backup and recovery, key and certificate update, and key history management are included in the major points to be addressed if a well-managed PKI is to be implemented. Retrieved on August 27, 2016 / <http://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf>).

PROPOSED SOLUTION TO THE PROBLEM

The current system only provides a hash value that would secure the integrity of the data. However, it lacks the security mechanism that would address confidentiality of the system which makes it possible for other servers aside from the official servers to exist in the transmission of the election returns.

As for the proposed solution this issue, a hybrid public key infrastructure has to be implemented to not only authenticate the data being transmitted but to also allow the verification of the server’s authenticity. The process will start once the voting period ends around 5:00pm of the election day. On the current system, the voting counting machine (VCM) will have to immediately send the election returns to the following servers: Municipal Board of Canvassers Server in the Consolidation and Canvassing System (CCS), Central Server, and Transparency Server. In the proposed system, the three said official servers will have to send an encrypted data to the VCM first with the use of the public key of the said VCM. This is to provide the VCM a go-signal to transmit the election returns. The VCM then will have to decrypt the data using its own private key to verify that the data was indeed from an authentic server in the system. Once the identification of the servers is verified, the VCM and the server can now create key exchange using the Diffie-Hellman algorithm that will yield its own generated key. Once a key is generated, this will be used to encrypt the election returns and send to the servers. The servers will have to verify the hash value of the election returns to know check the integrity of the data as well as its origin.