



Information security of the 2016 Philippine automated elections: A case study

Authors

Jeffrey Ian Dy, MSc (Royal Holloway, 2021)
Konstantinos Mersinas, ISG, Royal Holloway

Abstract

The Philippines will once again hold Presidential National and Local Elections on May 9, 2022. Philippine National Elections are fully automated with the Automated Election System (AES) supplied by Smartmatic since 2010. The upcoming election, however, is overshadowed by questions left unanswered from the 2016 presidential elections. We analyzed 426 log files provided by the Philippines' Commission on Elections (COMELEC) to objectively recreate what transpired during the 2016 elections. These log files were used to gauge the integrity of the Philippine AES using an AES Trust Model developed by this research. The model consists of eight properties that are considered universally applicable to any automated election, and based on the election event logs, the 2016 election failed most of the properties. Our findings, conclusions, and recommendations have been submitted to the Joint Congressional Oversight Committee on the Conduct of Automated Elections. But while the Committee is already deep in preparations for the upcoming elections, there is yet no committee report on the 2016 elections to date. ^a

^aThis article is published online by Computer Weekly as part of the 2022 Royal Holloway information security thesis series <https://www.computerweekly.com/ehandbook/Royal-Holloway-Information-security-of-the-2016-Philippine-automated-elections>. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at <https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/>.

Questions raised on the integrity of the past automated presidential election

On March 9 of this year, the Filipino people will once again vote to determine the next leaders of the Republic¹. In a country with approximately 67.5 million voters and a 75% voter turnout, this year's election is expected to be another blockbuster. However, this year's polls come at the heels of questions left unanswered about the integrity of Asia's first and only fully automated Presidential National and Local elections.

Barely two years after the last Presidential Elections, on March 6, 2019, the 23rd President of the Philippine Senate, Hon. Vicente Sotto III delivered a Privilege Speech alleging electoral sabotage and fraud during the 2016 elections. He presented evidence that election results were transmitted days before the polls officially started. He also showed access logs which would indicate that the election servers were remotely accessed from outside of the Philippines.

As if these allegations were not pressing enough, on March 14, 2019, the Senate President made an even more serious charge. He alleged that there was a "secret" 4th server transmitting results to the Canvassing and Consolidation Servers (CCS). The CCS are a group of computers whose primary task is to summarize the results transmitted by all 93,000 Vote Counting Machines (VCMs). In order to grasp the seriousness of this allegation, one must know the relationship between the VCM and the CCS as used in the Philippine Automated Election System (AES).

¹The Philippine legislature consists of two chambers, the Senate and the House of Representatives. The senate consists of 24 members and is elected nationally while the House of Representatives has more than 200 members who are called Congressmen and are elected locally per legislative district.

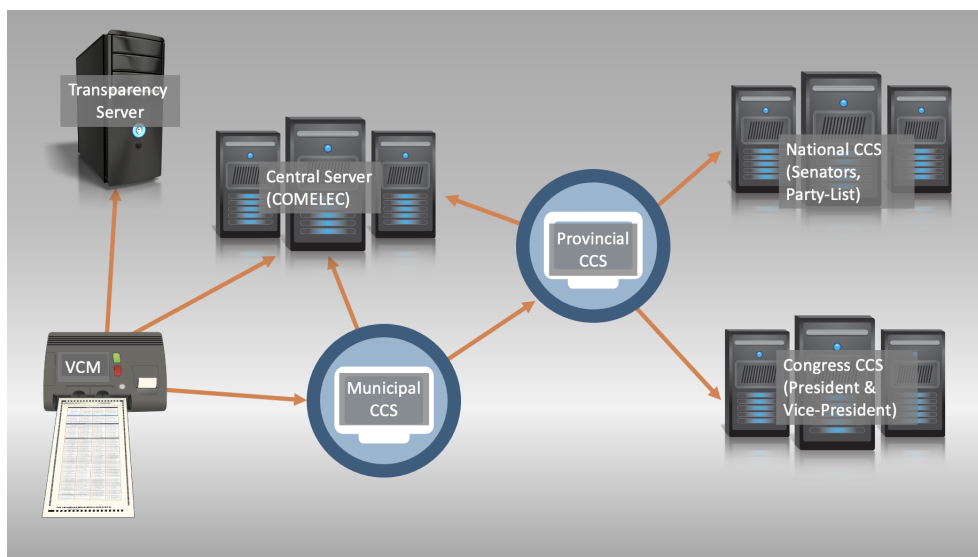


Figure 1: The VCM and CCS transmission hierarchy

The Philippine AES

Each of the 93,000 clustered polling precinct is assigned one VCM. The VCM's job is to accurately read each of the ballots fed into it. Once the polls are closed, the VCM produces what is called an Election Result (ER). As shown in Figure 1, the ER from the VCM is transmitted to three destinations: (1) Transparency Server, (2) COMELEC Central Server, and the first level CCS called (3) the Municipal or City CCS. Each VCM is associated to only one Municipal/City CCS, and a control mechanism must be in place to prohibit it from transmitting the ER to any other CCS. Meanwhile, another control mechanism should also be in place to ensure that the Municipal CCS can only perform the canvassing and consolidation of the ERs from VCMs located within its municipality. Otherwise, there will be a duplication of the counting of ERs.

Figure 1 shows the Municipal CCS transmitting its canvassing results to the Central COMELEC Server (indicated by the orange arrows), and to the Provincial CCS. This happens after the Municipal CCS finishes the canvassing of results of all ERs it expects to receive. Once done, it will produce the Certificate of Canvass and Proclamation (COCOP) showing the canvassing results and proclaiming winners in the municipal level (Mayors, Vice Mayors, Congressmen, City Councilors, etc.). It then transmits the canvassing result to the next level CCS in the hierarchy, usually a Provincial CCS. The process is repeated at the Provincial CCS level in the hierarchy. This process is again repeated all the way up to the Congressional CCS which canvasses and produces the results for the President and Vice-President.

Glossary

AES	Automated Election System
COMELEC	Commission on Elections
CCS	Canvassing and Consolidation Server
VCM	Vote Counting Machine
ER	Election Result

The Senate President's allegation about the presence of a 4th server was grave for two reasons. First, the existence of the 4th server transmitting ERs and/or canvassing results to other CCS alters the transmission flow and puts into question the security protocols to ensure that only specific VCMs and CCS should be able to transmit to specific CCS in each level of the transmission hierarchy. Second, Philippine Election Law requires that all elements of the AES should undergo a source code review both by an International Certification Entity (ICE), and local experts and political parties. The allusion that the 4th server is "secret" meant that it did not undergo the required review and evaluation.

The allegation is so grave that the same was used by the camp of former Senator Ferdinand “Bong-bong” Marcos, Jr. in his electoral protest against Vice President Maria Leonora “Leni” Robredo, which was filed before the Supreme Court sitting as the Presidential Electoral Tribunal. Marcos lost to Robredo in 2016 by a slim margin of 263,473 votes.

This year, the same protagonists Robredo and Marcos face off with other candidates for President. Unfortunately, questions on the integrity of the last Presidential and National elections continue to hound the upcoming polls. The Joint Congressional Oversight Committee (JCOC) was convened multiple times to investigate the allegations of the Senate President, but no committee report on the conduct of the 2016 election was published by the JCOC nor by the Senate.

Analysis and conclusions on the information security of the 2016 automated presidential and national elections

Permission was given by the Senate to analyze 426 log files submitted to the JCOC by the Commission on Elections (COMELEC). Python programs were written to parse through thousands of lines in these logs. The aim was to recreate the events of the election, and to see if the allegations of the Senate President can be proven. The results of the analyses were then considered to assess the trustworthiness of the 2016 Presidential Elections of the Philippines using an AES Trust Model developed by this research. The developed AES Trust Model has 8 properties, to wit:

1. **Voter privacy** refers to the property that assures the anonymity of the voter and the unlinkability of the votes cast to the voter.
2. **Uncoercibility/Receipt-freeness** is the assurance that a voter cannot sell his/her vote by providing proof to any party of how he/she voted.
3. **Individual verifiability** refers to the capability of the system to assure the voter that his/her vote was counted and processed as intended.
4. **Universal verifiability** is the assurance that the system follows the laws, rules and regulations governing the election. The assurance is based broadly on how transparent the system is when processing votes and how reproducible the results are.
5. **Fairness** is the assurance that no other party has the capability to know the partial count of the election while the polls are still open.
6. **Integrity** refers to the assurance that the AES can detect and recover errors, and that the entire system is tamper-proof.
7. **Availability** refers to the assurance that the election is resilient against attempts to derail it. This is especially important because elections are timebound and prematurely closing or disrupting elections results in voter disenfranchisement.
8. **Non-repudiation** refers to the assurance that an election official is indeed the same person who generated and transmitted the various reports that would become the legal basis for proclamation of winners.

These properties are widely accepted and each of them appeared in different scientific journals and academic research investigating the integrity of different AES.

The research has its limitations. The 426 log files available for analysis only represent 0.22% or 120,740 voters out of a population of 54.36 million registered voters. Thus, this could not be a statistical representation of how the entire election was conducted. In terms of scope, the log files consisted of 192 unique VCM log files corresponding to 192 clustered polling precincts for only 3 out of the 1,488 Municipalities in the country. Although there were VCM logs for 3 Municipalities, only 2 Municipal CCS logs were provided. The CCS logs were from the Municipalities of Libon in the Province of Albay (for VCMs whose ID started with 0507) and of Tugaya in the Province of Lanao Del Sur (VCM IDs starting with 3269).

An analysis of the available log files proved the existence of the “secret” 4th server, and transmissions

Table 1: Summary of findings for the 2016 Elections

#	Findings	Severity	Occurrences (% of the 192 VCMs)
1	Rezeros after actual votes counted	Critical	4 (2.08%)
2	CCS received results at an earlier time than VCM transmission time	Critical	13 (6.77%)
3	CCS successfully processed results not from the VCM IP address but from 10.101.1.198	Critical	22 (11.46%)
4	CCS successfully processed a transmitted result but VCM did not transmit	Critical	2 (1.04%)
5	VCM transmission successful but CCS did not receive the transmission	Critical	19 (9.9%)
6	Ballots inserted after the last counted ballot (uncounted ballot)	Major	20 (10.42%)
7	First ballot fed on May 9, but earlier than official election time	Major	31 (26.56%)
8	Transmissions made before election day (May 9, 2016)	Major	16 (8.33%)

indeed happened before the official opening of the polls at 7:00 am of May 9, 2016. Table 1 shows a summary of the critical and major findings.

The research also revealed other significant events that can prove useful in defining the control mechanisms needed to improve the information security of the 2022 Automated Elections. Event number 1 in Table 1 mentioned that 4 VCMs were “rezeroed”. “Rezero” is the term used by the VCM to indicate that actual votes stored in the machines’ removable storage devices were erased. These happened in 4 polling precincts in Tugaya, Lanao Del Sur, located at the southern part of the country. Table 2 enumerates the details of the rezeros.

Table 2: Details of rezero events in Tugaya, Lanao Del Sur

VCM ID	# ballots before rezero	Time of last ballot cast before rezero	Time of rezero	# ballots cast after rezero	Time of last ballot cast after rezero
36290005	256	2016-05-09 20:16:34	2016-05-10 21:30:06	329	2016-05-11 03:10:14.339
36290014	156	2016-05-09 14:37:07	2016-05-10 21:28:07	218	2016-05-11 00:40:22.101
36290016	442	2016-05-09 19:24:30	2016-05-10 21:35:50	654	2016-05-11 08:26:42.948
32690019	155	2016-05-09 13:38:11	2016-05-10 21:28:43	362	2016-05-11 03:26:28

Rezero events are considered “critical” for the following reasons:

1. There was no published rule from COMELEC authorizing a rezero.
2. The rezero done affected a significant number of ballots already cast.
3. There was a substantial discrepancy between the number of ballots read by the VCM before and after the rezero.
4. The rezeros happened very late in the evening of May 10, and ballots were recast until very early morning of the following day. Comparing the time difference between ballots fed, it is highly probable that the ballots were fed not by the voters themselves but by election officials. This weakened assurance of voter privacy and fairness in the AES Trust Model.

Apart from the rezero events, the elections held in Tugaya in 2016 were also suspicious. Of the 25

VCMs deployed in each of the clustered polling precinct in the Municipality, 19 successfully transmitted their ERs, while 6 did not. However, the Municipal CCS in Tugaya reported that it received only 3 of the 19 ERs transmitted by the VCMs. But the more surprising discovery made was that the 3 ERs received by the CCS were received not from the VCM's IP address, but from one single IP address, "10.101.1.198". Similarly troubling is that although received by the CCS from the same source IP address, the ERs were made to appear as if they still came from different VCM IDs.

This behavior was observed not only in the Tugaya CCS but in both CCS logs made available to the JCOC. In both CCS logs, transmission of ERs from the said IP address appeared 78 times, of which 22 were processed successfully. This behavior was what was being referred in event number 3 in Table 1.

Fifty-six (56) transmitted ERs from 10.101.1.198 were discarded by the two CCS because they already received an earlier transmission from that of the original IP address of the respective VCMs. Table 3 shows a sample of the IP addresses of the 22 VCMs that transmitted and what IP address the CCS received.

Table 3: CCS successfully processed 22 transmissions not emanating from the VCMs registered IP address: a sample

VCM ID	VCM Transmit IP	CCS Received IP	Transmit Received (CCS)
05070002	10.11.98.105	10.101.1.198	2016-05-09 17:50:23
05070014	10.12.83.240	10.101.1.198	2016-05-09 18:39:51
05070019	10.12.60.201	10.101.1.198	2016-05-09 20:00:11
		⋮	
36290020	10.12.123.72	10.101.1.198	2016-05-10 07:55:04

Event number 3, when taken collectively with events 2, 4 and 5 (refer to Table 1), proved the existence of the so-called 4th server. For example, event number 4 in Table 1 referenced 2 transmissions received by the CCS in Libon (CCS ID 0507), even though the same 2 VCMs (VCM ID 0507012 and 0507013) did not successfully transmit its ER. This is the opposite of what happened in the Tugaya CCS (CCS ID 3629). In the latter, 3 transmissions made by the VCM were received by the Tugaya CCS, But the CCS received it from a different IP address. Despite this difference, the outcome was the same, they both received a transmitted ER from 10.101.1.198 which is different from their VCMs' registered IP addresses.

One might think that 10.101.1.198 is Network Address Translation (NAT) IP address, but evidence showed it was not. In this case, there are VCMs that did not transmit, but their corresponding CCS received a transmission from 10.101.1.198. In addition, there were 56 instances when a transmission was received from 10.101.1.198, yet the CCS also received the same election result from the same VCM ID, but from their respective 'original' IP addresses, as reflected in their respective VCM log files. NAT IP addresses cannot co-exist with the IP addresses of the different network elements behind the NAT interface. This is simply not possible. Thus, this is incontrovertible evidence that 10.101.1.198 is not a NAT IP address.

The presence of the computer with IP address 10.101.1.198 places COMELEC in a difficult position where any offered explanation will lead to an unsatisfactory result. During one of the hearings of the JCOC, when the earlier versions of this research were presented to the panel, COMELEC already admitted the existence of the 4th server but downplayed its role in the election as simply a "routing server"². However, more recent analysis, especially those made in the full MSc dissertation on which this article is based, showed that 10.101.1.198 cannot be simply a routing server. It should be reiterated that there were instances when no transmissions were made by the VCM yet 10.101.1.198 transmitted an ER, and the CCS processed it. Where could the Election Results (ER) have come

²"Transcript of the June 4, 2019 hearing of the Joint Congressional Oversight Committee on the Automated Election System," in Joint Congressional Oversight Committee on the Automated Election System, 17th Congress, 3rd Regular Session ed, 2019.

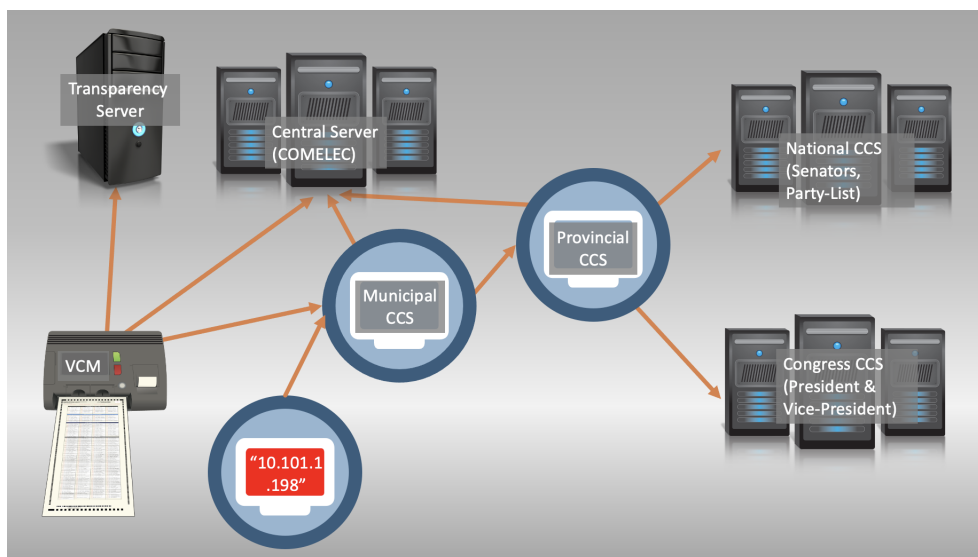


Figure 2: 10.101.1.198 altered the transmission flow and puts doubt on the control mechanism in place against double-counting of ERs

from? It should also be noted that the VCMs are identified by their VCM IDs. According to public pronouncements of both COMELEC, Smartmatic, and the ICE certification³, the CCS will only process results from specific VCMs that fall within its jurisdiction. This behavior is important because it is the assurance that the entire AES supplied by Smartmatic, Inc. will not “double count”. The existence of 10.101.1.198 which apparently can assume the VCM ID of any VCM and thus transmit to any CCS puts into question the protocol and control mechanisms in place to ensure that CCS will only process results from identified and legitimate VCMs within their respective jurisdiction. It appears 10.101.1.198 is a super VCM that is allowed to transmit to any of the more than 1,500 CCS used in the 2016 elections. A computer found in the AES that behaves like 10.101.1.198 were never present in the ICE reports, nor was such a computer ever mentioned nor presented in any of the local source code reviews⁴. Unfortunately, these questions were never fully answered because the AES used by the country is proprietary, and its copyright owner Smartmatic, Inc. refused to publish the information security protocols of the AES used in Philippine elections.

Due to the foregoing reasons, the AES used by the Philippines in 2016 failed in five (5) out of the 8 properties of the AES Trust Model. It failed in the properties of (1) Individual Verifiability; (2) Universal Verifiability; (3) Fairness; (4) Integrity; and (5) Non-Repudiation. Other findings, sources, and full details of the research can be accessed at <https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/>.

Biographies

Jeffrey Ian Dy graduated MSc in Information Security with Distinction at the University of London in 2021. He was invited multiple times as a member of the Technical Working Group, and resource person for the Joint Congressional Oversight Committee on the conduct of the Automated Elections in the Philippines. Currently, he is the Director IV for the ICT office, and concurrently the Regional Director for Cordillera Administrative Region of the Technical Education and Skills Development Authority (TESDA), a Philippine government agency tasked to direct, promote, develop and regulate programs and standards geared towards a quality-assured and inclusive technical education and skills development and certification system.

Konstantinos Mersinas, PhD, CISSP, is an Associate Professor at the Information Security Group at

³S. G. Solutions, “Final Certification Test Results Comelec AES 2016 Voting System,” April 14, 2016.

⁴“Transcript of the June 4, 2019 hearing of the Joint Congressional Oversight Committee on the Automated Election System,” in Joint Congressional Oversight Committee on the Automated Election System, 17th Congress, 3rd Regular Session ed, 2019.

Royal Holloway, University of London. Konstantinos has worked in various information security industry roles before moving to academia. A trained mathematician, his research interests lie with behavioural and experimental economics in cybersecurity, decision-making, and cybercrime. Konstantinos co-founded the interdisciplinary research group HIVE to bridge psychology, law and cybersecurity. His research has been funded by the National Cyber Security Centre in the UK.

Series editor: S.- L. Ng