Election Petition ICT Experts Report - What You Need to Know

Liban Hannan (InformAction)

07/09/2017

Contents

Introduction

On August 29th, 2017, as part of the petition challenging the credibility of the presidential election, the Supreme Court of Kenya ordered the IEBC to allow scrutiny of its servers[See Order A]. This order was meant to facilitate an investigation of the integrity of the IEBC systems that were used to transmit and receive results. Overall, the scrutiny results indicate whether the systems may have been compromised and whether they met legal standards for the conduct of elections.

This report shows that IEBC's non-compliance with the order scrutiny of its ICT was extensive and prevented the court from examining what happened on IEBC networks, servers, and equipment in a pattern that looks like obstruction.

This report has been written without access to the annexures of the ICT Experts' report.

Analysis

The orders referred to below are explained in the *Orders* section

Basic information about IEBC Systems

Orders A, B, and C:

A, B, and C would provide the court with a picture of what sort of traffic was allowed on IEBC's network, how many servers were on that network, and what operating systems those servers were running. This information would give an idea of which points of entry an attacker could use, and which servers may have been vulnerable.

Notably, IEBC was not required to disclose the version of the software it was using, or the configuration details of the external firewall. This makes it hard to ascertain how an attacker would have accessed the network, and what vulnerabilities they would have exploited[See Order B].

However, had IEBC complied with order B, it would at least provide information on which services might be exposed if another was hacked. e.g Attackers might use compromise of IEBC's website to gain entry to the commission's networks, then launch attacks on other servers. This could be prevented by a firewall blocking traffic between servers that do not need to communicate. Poorly configured internal firewalls can allow even more worrying access, such as exposing servers to WiFi users, who come and go and are often unverified or guests.

The court excluded software versions to protect the security of IEBC systems.

Take away: IEBC seemed to assume that it would not have to provide information if it didn't want to. The court was prevented from knowing how exposed IEBC's server's were to attacks.

Who Had Access To The Systems?

Orders D to F, and L:

These orders allowed the court to determine who had access to the system, the extent of that access, and what people could do. D to F reflect internal access (passwords, user types, etc.), while L reveals which third parties had external access to the system via one API[See Order L]. The petitioner's request for a list of all APIs suggests that there could be other access points not seen by the court.

Take away: The court was able to discover who had internal and, to a lesser extent, external access to the system. It is not clear if all external access points were disclosed.

What Were IEBC's Plans To Deal With Technology Failures And Problems?

Order G:

It is notable that IEBC only provided a Disaster Recovery Plan, and not a Business Continuity Plan. The Business Continuity Plan would be considered essential by many for an operation like the election, and is a source of serious concern that it wasn't provided.

Provision of the Disaster Recovery Plan means that they had procedures in place for a disaster (e.g. extensive failure of transmission), but no formal plans to prevent more predictable challenges they were likely to face (e.g. server failure).

Take away: IEBC complied with this order but their partial compliance and omission of a Business Continuity Plan highlighted a large gap in in their preparations for elections.

Were IEBC's Systems Secure?

Order H:

Order H requires IEBC to hand over reports on penetration tests on the IEBC's systems. Penetration tests involve cybersecurity professionals assessing the integrity of systems by attempting to gain entry to them. These are required by law to be certified by "a professionally reputable firm". IEBC appears to have either self-certified these reports or has no certification at all.

This is a clear breach of The Elections (Technology) Regulations 10(2), 2017.

Take away: IEBC went into the general election without verifying that its systems were secure. The IEBC's pre-election assurances to the public about systems security were dishonest; without proper tests, the Commission had no way of knowing how secure (or not) the ICT systems were.

Where Did The KIEMS Kits Transmit From?

Order I:

Order I required IEBC to provide location data from KIEMS (Kenya Integrated Election Management System) kits. KIEMS kits would be expected to only be near polling stations or near agreed locations where mobile internet is available for transmission of data.

IEBC provided the GPS locations of polling stations but not those of the KIEMS kits. The reason for this error was not explained, by IEBC; it drastically limited the court's picture of how the KIEMS kits were used on election day. Combined with Order J, where IEBC does not provide a "comprehensive" list of which KIEMS kits[1] were unused and/or un-deployed, it is alarming that we know so little about which KIEMS kits were used and where. This is despite IEBC being able to provide this information.

Take Away: We do not know where the KIEMS kits were on polling day. We also cannot determine whether any KIEMS kits were used, but should not have been. This means malicious actors could use unallocated KIEMS kits from a single location to transmit forged form 34As, for example, and we would not be able to identify them.

User Activity on IEBC Systems

Order M, N, and O:

In these orders, IEBC was asked to provide log-in trails of user and equipment to IEBC's servers and KIEMS Database Management Systems. The log-in trails are essentially a list of who and what accessed the IEBC's systems and when.

[1] IEBC is ordered to provide a certified list, they provide a spreadsheet.

Worryingly, IEBC only provided a softcopy of the logs with no attempt to demonstrate they originate from the systems in question. This means there is no guaranteed link between what IEBC provided and the servers they claimed to be providing them from. This would leave room for tampering with the logs before they could be scrutinized.

A log-in trail is usually an effective way of finding suspicious activity. It is common that intruders or rogue users will tamper with log-in trails to hide their activity. That IEBC obstructed retrieving these logs directly from the servers (deliberately or otherwise) prevents the court's ability to know with certainty what happened on IEBC's systems.

Non-compliance with Orders M,N and O meant that Order P cannot be complied with.

Take Away: IEBC's non-compliance means we are prevented from knowing much about what happened on IEBC's servers during the election process. Further, IEBC's behaviour regarding orders M, N, and O looks like an attempt to hide information.

Technology In The Court

Over the course of the petition lawyers often struggled with technical terms and issues, especially those for the Petitioner and 1st Respondent. Frequently speakers got bogged down in technical detail without adequately explaining the meaning of those details outside of an ICT context; or, the implication of a finding was presented as if self-evident.

This was particularly obvious in the comments on the ICT experts report. James Orengo (lawyer for petitioner) listed findings from the report without explaining their meaning – for example, he emphasized there were "deletions" of images discovered on the IEBC servers , but did not explain why he thought why that was significant. Deletion, which sounds naturally alarming, is often performed for legitimate reasons e.g to remove duplicate images in the event of a KIEMS kit transmitting multiple times. IEBC asserted prior to the election that it was not possible to do a re-send by the user; but, in terms of the actual transmission, the KIEMS kit would almost certainly re-try in the event of a failed transmission.

Lawyers for the IEBC attempted to use the inaccessibility of technical details to disguise their client's obstruction or shortcomings e.g Paul Muite (lawyer for 1st respondent) described the difficulty of "getting around the firewall" as if it were a physical wall, rather than standard access control technology.

The combination of delays around the scrutiny as well as the pressure to hastily compile and distribute the reports, meant the implications and impact of the scrutiny was not necessarily immediately or fully harnessed – either by all in the court, or the public.

Summary Of IEBC Compliance With Supreme Court's Orders

	List of orders	Total
Complied fully, no objections	A, D, E, F, H[2], K	6
Complied fully, with objections	C[3]	1
Complied Partially	G[4], J[5], L[6]	3
Did not comply	B[2], I[7], ^M, N, O, P	6

Total orders: 16

IEBC complied fully with less than half the orders in the scrutiny (7/16). It is not indicated in cases of partial compliance whether the requested documents were available but not supplied.

Orders

This details and explains the orders given. Some of the orders below have been paraphrased.

A: Information about the number of servers in IEBC's exclusive possession.

In this context a server is a computer that provides one or more services to clients (the public, other computers, the press, etc.). In the case of the Results Transmission System these services would probably be spread across multiple servers and include web, database, and storage services among others. *System* and *service* are sometimes used interchangeably.

This order is for IEBC to provide information on all the servers IEBC possesses but is not explicitly limited to those providing the collection.

Compliance: Yes.

Information available: No, annexures not available. Comments provide no extra details.

B: Firewalls (without the disclosure of software version).

Firewalls control the flow of traffic on a network. They determine which types of traffic are allowed, from which sources they're allowed, and the destinations they're allowed to go to.

The petitioner requests the configuration of the internal and external firewall. The meaning of external firewall controls traffic flowing between IEBC's internal network and the internet. However the meaning of internal firewall is less clear. It likely means the firewall controlling what traffic can flow within the IEBC's different parts of IEBC's internal network.

Compliance: No. IEBC provided a diagram instead of the actual configuration of of the firewall.

[2]IEBC found to be in breach of elections regulations
[3]Petitioner requested more information
[4]Partial compliance not objected to
[5]Provided a spreadsheet, not a certified list
[6]Did not provide a list of APIs, petitioner's request for list considered unclear
[7]IEBC is ordered to provide a certified list, they provide a spreadsheet.

Information available: No, annexures not available. Experts indicated IEBC could provide information on the internal firewall without compromising its system's security, but allowed that disclosing external firewall configurations was a security risk.

C: Details of operating systems used on IEBC servers (without the disclosure of software version)

Investigators must know what operating systems are in use to ensure they have people with the right expertise doing the analysis. Operating systems are responsible for managing how a server's resources (primarily processing power, storage, and memory) are used, and controlling access to resources and software. Approaches to security vary significantly between different types of operating systems.

Compliance: Yes, petitioner requested more information.

Information available: No, annexures not available. Comments provide no extra details.

D: Password policy

A password policy normally consists of a written list of rules about how users should construct and manage passwords to maximise security. This is normally part of an organisation's official regulations. This may include things like not using easily obtainable personal information (name, date of birth, names of close family members, etc.), how frequently passwords must be changed, whether passwords can be shared and who they can be shared with.

Compliance: Yes.

Information available: No, annexures not available. Comments provide no extra details.

E: Password matrix

This is not a common phrase, but might be a list of users and what they can access.

Compliance: Yes.

Information available: No, annexures not available. Comments provide no extra details.

F: System user types and levels of access.

Many operating systems express access to data through "privileges". A privilege in this context is the granted ability to do a specific type of action. e.g. If a user has "read" privileges on some data, that user can read the contents of that data. If a user has "write" privileges on some data, the user can (depending on the operating system) change the data in any way they like (append, delete, replace, etc.). Should a user try to perform an action that they do not have the necessary privileges to do, they will receive an error message.

A system user type can be thought of as a named bundle of privileges used for a specific purpose. These can be assigned to a user e.g. the user "Kamau" is assigned the "Printer Maintenance" system user type. This grants Kamau the privileges necessary to carry out standard printer maintenance task.

Compliance: Yes

Information available: No, annexures not available. Comments provide no extra details.

G: The IEBC Election Technology System Redundancy Plan, comprising its Business Continuity Plan and Disaster Recovery Plan.

A Business Continuity Plan consists of the measures put in place to ensure systems keep running under various scenarios - power loss, server failure, staff loss, civil unrest, etc.

A Disaster Recovery Plan is how an organisation will deal with disasters with respect to their computer systems. This would address how IEBC expected to recover from incidents where widespread failure occurred (e.g. due to extensive data loss, capacity loss, software failure, or sabotage).

Compliance: Partial. The Business Continuity Plans was not provided. This omission is not explained by the experts, or objected to by the petitioner.

Information available: No, annexures not available. Comments provide no extra details.

H: Certified copies of certificates of Penetration Tests conducted on IEBC's systems

A penetration test is usually conducted by a cyber-security professional and consists of attempts to gain access to systems in an adversarial manner. The methodologies used are chosen to mimic typical behaviour by attackers attempting to gain unauthorised entry. The aim of these exercises is to find entry points and exploitable weakness in systems so that they can be fixed before a real attacker can use them.

Compliance: Yes

Information available: No, annexures not available. Petitioner and experts commented on provided information being in breach of The Elections (Technology) Regulations 10(2), 2017.

I: GPRS location of each KIEMS kit used during the Presidential Election from 5th to 11th August

The location of KIEMS kits from polling day to the declaration of results as reported by their GPS sensors.

An error is made in this order. GPRS is a mobile internet technology (how mobile phones connect to the internet), GPS is a location technology – they are unrelated technologies with different purposes and similar names. However it is clear from the mention of "location" that GPS is meant. It is a common point of confusion.

Compliance: No. Incorrect document provided

Information available: No, annexures not available. Comments provided no extra details beyond indicating that IEBC should have provided the correct document.

J: Certified list of all KIEMS kits not used and/or deployed during the Election

This order is ambiguous. Does it mean kits not used but deployed, or does it mean not used and [not] deployed? It is likely to be the latter.

Compliance: Partial. Spreadsheet provided instead of "certified list".

Information available: No, annexures not available. Comments indicate that there were no objections to receiving a spreadsheet instead of a certified list. Experts commented that the documentation was not comprehensive.

K: The polling station each KIEMS Kit was allocated to

This order sought to know where each KIEMS kit was supposed to be on polling day.

Compliance: Yes.

Information available: No, annexures not available. Comments provide no extra details.

L: Technical Partnership agreements IEBC had for Election Technology Systems, including disclosure of APIs used for data exchange as a list

An API (Application Programming Interface) is a collection of commands that programs can give to IEBC systems to obtain data in a format that is easy to process with programs, and potentially modify data (depending on the purpose of the API).

APIs dictate how external users can interact with a system. This may involve access to information, commands to modify the system, or both. Auditing APIs is important to find possible integrity issues. E.g. an API for results data might allow the user to make the system unavailable, or worse, change the data on the system.

The definition of "technical partner" is unclear and may extend to contractors that had access to IEBC's systems.

Compliance: Partial. IEBC provided a link to *one* API, and did not specify if that was the only API used. The order was for a list of APIs. This may have lead the petition to believe there were more APIs for the Election Technology System.

Information available: No, annexures not available. Comments suggest petitioners request was not clear.

M: Log in trails of users and equipment into the IEBC Servers

This is a list of which users and equipment (e.g. KIEMS kits) logged into IEBC servers, what time they logged in, and (depending on the interpretation of this order) what those users or equipment did.

Compliance: No. IEBC provided a copy of the logs on a hard disk.

Information available: No, annexures not available. Comments show that IEBC did not provided access to systems as ordered, and failed to demonstrate the origin of the information they provided on the hard disk.

N: Log in trails of users and equipment into the KIEMS Database Management [System]

As in Order M above, but for the KIEMS Database Management System

Compliance: No. IEBC provided a copy of the logs on a hard disk.

Information available: No, annexures not available. Comments show that IEBC did not provided access to systems as ordered, and failed to demonstrate the origin of the information they provided on the hard disk.

O: Administrative access log into the IEBC public portal from 5th to 29th August

This order is awkwardly phrased but can be taken to mean - a list of times when a user with administrator privileges logged into the IEBC public portal, and what they did. Administrator privileges grant a user the right to modify a system extensively.

Compliance: No. Compliance with order P is impossible without complying with orders M, N, and O.

Information available: No, annexures not available. Comments show that IEBC did not provided access to systems as ordered, and failed to demonstrate the origin of the information they provided on the hard disk.

P: A soft copy of the logs required in orders M, N, and O

Compliance: No. Compliance with order P is impossible without complying with orders M, N, and O.

Information available: No, annexures not available. Comments show that IEBC did not provided access to systems as ordered, and failed to demonstrate the origin of the information they provided on the hard disk.

Follow up

Areas of concern:

- IEBC's non-compliance regarding activity logs (orders M, N, O, P) looks like an attempt to hide information
- IEBC asserted its systems were secure during the election period despite being in breach of regulations that required it have the security of its systems independently verified.
- IEBC's instances of partial compliance and non-compliance prevented the court from discovering important information about exactly what happened on IEBC systems over the course of the elections
- There is a high chance that further illegalities will be revealed in the information provided in response to the orders, which is not currently available
-

It should also be noted that:

- Legal teams in the petition appear to lack effective strategy for effectively communicating technical details to the court and the public
- There is need for Civil Society to ensure that it has the capacity and expertise to participate or engage in any further scrutiny of IEBC ICT systems, as this is key to understanding the failure and illegalities of the election