2023

Threat Analysis Report: Voting Systems

CS1STF

GEORGE HOTTEN

ASSESSMENT DECLARATION

I declare that I have personally prepared this assignment. The work is my own, carried out personally by me unless otherwise stated and has not been generated using paid for assessment writing services or Artificial Intelligence tools unless specified as a clearly stated approved component of the assessment brief. All sources of information, including quotations, are acknowledged by means of the appropriate citations and references. I declare that this work has not gained credit previously for another module at this or another University, save for permitted elements which formed part of an associated proposal linked directly to this submission.

I understand that plagiarism, collusion, copying another student and commissioning (which for the avoidance of doubt includes the use of essay mills and other paid for assessment writing services, as well as unattributed use of work generated by Artificial Intelligence tools) are regarded as offences against the University's Assessment Regulations and may result in formal disciplinary proceedings.

I understand that by submitting this assessment, I declare myself fit to be able to undertake the assessment and accept the outcome of the assessment as valid.

ASSESTS WITHIN THE VOTING SYSTEM

Within the UK voting system, there are several crucial assets that make the voting fair and integral. Not all these assets are secure against an attack. In this report I will present the numerous assets and explain how they could be vulnerable because of the many flaws within the UK voting system.

YOUR VOTE

The most important asset within the voting system is your vote itself. This is how you contribute to the country's democracy and have your say for its future. Ensuring this asset is not tampered with is the highest priority and keeping it safe helps prevent a breach of confidentiality and integrity.

BALLOT PAPER (AND POSTAL VOTES)

The ballot used to cast your vote is another important asset. Keeping the integrity of these ballots ensures that they cannot be easily forged, allowing for someone to vote more than once, and to ensure that no more ballots are produced than the exact amount required for each person's vote.

BALLOT BOXES

Ballot boxes are used to store people's votes before they are taken to a counting station. It is vital that these boxes are properly protected, and access is not given to any individuals until it is time to count the slips inside. If they are not secure, the integrity of the voting would be breached.

ELECTORAL ROLL

Each voting station will have a printout of the names and addresses of the constituents that will be voting at the station. It is important to ensure that there is no way to tamper with the information on that sheet, as this could lead to having more votes than permitted per person. The confidentiality of this sheet must also be always protected to prevent any breaches to people's privacy.

THE VULNERABILITIES AND THE THREATS

BALLOT PAPER ABUSE

COUNTERFEIT BALLOTS

One major vulnerability is the standardisation of the ballot paper used for each election and the fact that no identification is put on them. Whilst the lack of identification may help against attacks on specific voters and helps maintain confidentiality, this could lead to the threat of someone voting multiple times.

Each ballot has a standardised form of each candidate in a list, with their corresponding party's logo and a box to mark for if they have your vote. This could allow an attacker to potentially create multiple counterfeit ballots and use them to rig the election so the candidate of their choosing can win. The information needed to ensure the ballots are accurate could easily be gathered by someone willing to sacrifice their vote and smuggle their ballot paper out of the polling station and to the malicious individual. With the ballot paper out of the voting station, the malicious individual could easily create copies of the paper and use them when they go to vote themselves.

CORRUPT STAFF AT THE POLLING STATION

Another vulnerability is the staff that work at the polling station. The staff must have a level of integrity to ensure that they mark off a person's name when they visit the station, and to provide them with only one ballot paper. If they are not integral, this could further lead to the threat of someone voting multiple times.

A member of polling station staff who is working the morning shift could be bribed to not mark a voter's name of the electoral roll paper. This would allow them to cast their vote and then return later in the day when another member of staff is on shift who, as their name is not crossed off, would let them cast another vote. This creates a threat to the system as the integrity of the votes would be in-question as fraudulent votes would be counted as genuine.

THE CONTROLS

In attempt to prevent fraudulent votes, one control method could be to only produce the amount of ballot papers required for everyone to vote once. This would ensure that multiple ballots could not be handed out as it would mean genuine votes would not be able to cast their vote and would flag up that fraudulent activity may have occurred. To add to this, the number of ballots used should be comparted to the amount of people who voted which would prevent the use of counterfeit ballots as if more ballots were present than the amount of people who voted, this would be a major indication of fraudulent activity.

BALLOT BOXES

THE SEAL AND CORRUPT STAFF

Another vulnerability is the security of the ballot box holding the votes. If not properly protected, the box could be opened and ballot papers could be added, modified or removed, which causes a threat to the integrity of the votes and the election.

There are numerous points at which the ballot box could be vulnerable, such as in transport to and from the counting stations, and whilst at the polling station. At the counting stations, votes could be added or removed by corrupt members of staff in attempt to rig the election. The box could also be attacked whilst its at the polling stations, with members of staff also potentially removing or modifying votes.

THE CONTROLS

To prevent the box from being opened and any fraudulent votes added, the box should be sealed before it leaves for the polling station from the counting station. On this seal, there should be a unique number or marking which would be able to indicate if the seal has been broken, or if a new one has been applied. This should be noted down before it leaves the counting station and when it arrived back at the end of the day, this marking should be compared to ensure there has been no fraudulent activity. In addition to this, the above counting of the number of votes should also be used in case any fraudulent ballots were added during transport.

ELECTORAL ROLL

FAKE IDS

At the polling station, staff are checking for the name, address and photo on a valid identification card. However, there is no check to ensure the authenticity of the ID you are presenting. This vulnerability creates the threat of potentially being able to vote as someone else, allowing you to obtain more votes.

With a good fake ID, staff may not be able to pick up on fraudulent activity, allowing you to vote as someone you're not. As all that is required on the ID is your address, name and photo, a malicious acter could create fake IDs with the name and address of people they know, such as neighbours or friends. With their photo attached, it would allow them to vote under someone else's name.

This threatens the integrity of the vote as people would be able to vote multiple times under the different names. This also threatens other voter's confidentiality as their personal information is being found and used to commit fraud, potentially putting them at risk as well.

THE CONTROL

To prevent the use of fake IDs, the identification number of a drivers license or passport should be included on the electoral roll. This adds an extra layer of security for the staff members to check and, as these would be impossible to guess, it would prevent a malicious actor from being able to vote as someone else.

REGISTERING AT MULTIPLE STATIONS

As the electoral roll is managed per polling station, there would be nothing stopping a malicious acter for registering to vote at another station, which would allow them vote twice. This vulnerability creates the threat of potentially being able to vote numerous times at different polling stations. This threatens the integrity of the polling as people would be able to vote multiple times, making the ballot unfair.

THE CONTROL

To prevent the ability to vote at multiple polling stations, there should be a global system in place that unifies all the polling station's electoral data that is able to check to see if someone is already registered within the UK or their constituency. If they are, they should not be allowed to register at a new polling station.

CONCLUSION

Overall, the biggest threat to the voting system is the potential use of counterfeit ballot, as these can cause breaches to the availability and integrity of the voting. At the cost of protecting confidentiality, there is no uniquely identifiable information on the ballots meaning that counterfeits could be created and used if the proper protection is not implemented. Compared to other methods, counterfeit ballots are the largest threat as:

- Fake IDs: would cost a lot of money and would need in-depth knowledge of other people in your area.
- Registering twice: higher chance of getting caught as your name will be on all the documents.
- Corrupt Staff: would most likely require a bribe, and attempting to bribe the wrong person would get you caught.

Counterfeit ballots would require a minimal amount of setup, potentially only requiring a printer, and it would be easy to smuggle them into a polling station. They would also be highly distributable allowing for hundreds of people to print and submit fake ballots.

Total word count: 1533