INFO 679: INFORMATION ETHICS

FINAL PAPER ON ETHICS IN ELECTRONIC VOTING SYSTEM

KAVYA KUMAR

STUDENT ID 14313206

DREXEL UNIVERSITY

Introduction

In this paper, I will first describe about the ethical issues related to the electronic voting system. In the second section, the ethical principles that are required to make the electronic voting process reliable and secure are discussed. In the third section, the security requirements that must be attained to achieve the ethical principles in the process is explained. In the last section, the ethical dilemmas and the questions that arises as a result of ethical issues are discussed.

1. Ethical Issues related to electronic voting system:

As said by Katherine O’Keefe and Daragh O Brien, any information that is processed, except a few, affects the people in some or the other way. In the context of electoral process, information that is processed plays a vital role since the result of the process depends solely on the information processed. Hence it is essential to incorporate ethical measures by every individual involved in the election process to deal with the information and the systems used ethically.

The ethical issues from the perspective of a voter in the election process: The issues included are trust, proof of vote and rights of the voter.

Trust: For any electronic voting system to be effectively considered in electoral process, it is important that it gains the trust of the voters. Building trust takes several years of efficient and reliable operation of the system and it doesn’t arise spontaneously. It is not enough if the system is reliable, it is important that people believe that the system is reliable (Pieters, W. & Becker, M. J., 2005). Unless and until people believe that the system is reliable, there will be issues and arguments requesting for the investigations. Users on the internet seek anonymity to protect their privacy even while accessing a website or for everyday operations. It is obvious that for sensitive process like elections, voters require anonymity to prevent themselves against political distress. This allows the voters to vote more politically correct. This can be achieved when voters believe that their anonymity is protected. Hence designers and policy makers have 2 responsibilities: one to make sure that the system protects the anonymity of the voters and the other is to make sure that the voters believe that their anonymity is protected (Pieters, W. & Becker, M. J., 2005).

Proof of vote: As the name implies, proof of vote deals with the evidence for the voter that the vote they casted is same as that is recorded in the electronic system used in the electoral process. This proof is a vital component in building the trust of the voters. There are several ways in which the proof could be provided. Say for example, a receipt given to the voters after the voting process. But there are several unethical consequences after the receipt has been provided. One such consequence is vote selling for political advantage. Also, an attacker could eavesdrop and know the vote the voter casted and could threaten him. In this context, there arises an ethical question: “Isn’t this a violation of the voter’s right to verify the vote he/she casted?”

Rights of the voter: In the voting terminals, there are several softwares that are installed to facilitate the electronic voting process. Some of these software programs’ source code are not available to the general public. One of the main reasons why the programs are not disclosed to the public is due to the fact that they might motivate the attackers to find and exploit the vulnerabilities in the system. But there arises an ethical question: “Isn’t this a violation of the citizen’s right to verify the voting process completely?” (Pieters, W. & Becker, M. J., 2005). It is not impossible to completely test the voting system for possible vulnerabilities and then implement it in the electoral process. But even after ethical hacking and penetration tests, there could be a slightest vulnerability found. As we know, e commerce applications are vulnerable to attacks because of increasing hacker communities. Also, when it comes to testing the electronic voting system, there arises several ethical issues from the perspective of researcher that are discussed in the next segment.

Phase I: Obtaining required information by the researcher

There are three main ways through which a researcher could obtain information about the voting system. They are:

1. Through leaks and anonymous sources.
2. From government sponsored studies.
3. By purchasing government surplus machines. (Robinson, D. G., & Halderman, J. A., 2012).

There are ethical concerns associated with the ways used to obtain the information. When considering the first case where the researcher obtains the information from anonymous sources, it is important to know if the source is lawfully permitted to provide the information. Also, it is important to think about who is responsible if the information is misused by the researcher. In case of leaks, researchers obtain the source code or if the source code is not available, researchers use reverse engineering techniques to obtain the technical information needed. There arises an ethical issue about if it is ethical according to the intellectual property protection to use reverse engineering techniques or source code without authorization. Also, once the information has been obtained, it is important to think about how a researcher should react or go about the problems that arises when they access the information from the sources that are not officially legal or approved (Robinson, D. G., & Halderman, J. A., 2012).

Phase II: Analyzing the obtained information to find security issues.

Researchers analyze the information obtained about the system to find the vulnerability. This security analysis includes understanding the functionality of the system, performing ethical hacking and penetration testing to find the possible vulnerabilities. It is important to learn about the ethical issues during this phase. One of the issues arises due to the presence of confidential data of the voters during the analysis of the voting machine. For example, in the research study of Indian voting system, the systems used by the researchers contained the election data of the previous year. In such cases, researchers must handle the systems cautiously and protect the voter information from being leaked for passive attacks such as for analyzing the voters’ likelihood for choosing a particular political party (Robinson, D. G., & Halderman, J. A., 2012)..

Phase III: Disclosing the vulnerabilities found after analysis

Another essential analysis is when the vulnerability has been found. It is crucial to think if it is unethical for a researcher not to disclose the vulnerability to the public. When we think from the perspective of researches, there are several ethical dilemmas a researcher could face when they think about disclosing a security issue in the voting system. A single group of researchers cannot guarantee that they have found all the possible vulnerabilities in the given system. It is almost close to impossible for any researcher to detect every vulnerability at once. Hence, these evaluations could allow the vendors or voting officials to correct the problems mentioned and claim that the systems are completely secure. This could be a false sense of security among the voters which is not ethical. Also, the vulnerabilities if disclose could motivate the attackers to exploit them before it is considered by the voting officials or could have immediate effects on the voter confidence and turnout. It is also possible that the researchers could face potential harm like physical abuse that might hold back them from disclosing the security issue of the system (Robinson, D. G., & Halderman, J. A., 2012).

1. Ethical principles of electronic voting system:
2. In order to ensure that the results of the voting process is reliable it is important to ensure that only eligible voters are allowed to vote and that they vote only once.
3. In the process of counting votes, it is vital to ensure that all valid votes are included and invalid votes are excluded from the count.
4. Verification the vote of the voter i.e., to ensure that the vote that is recorded in the system is exactly the same that is intended by the voter.

Also, most important principle is to protect the secrecy of the votes. This means that it must not be possible for anyone to derive the relation between the vote and the voter and there should not be any proof that the voter has voted. This prevents the sale of votes for political misuse (Pieters, W. & Becker, M. J., 2005).

1. Requirements to achieve the ethical principles:
2. Privacy: Privacy is achieved when there is a private link between the vote and the voter (Nguyen, T. A. T., & Dang, T. K., 2013). This can be very well understood by the differentiating the electoral process with the banking process. In banking, the user is first authenticated, and the transaction is linked to their personally identifiable information. Where as in the case of electoral process, the user is authenticated but the transaction is not linked to their personally identifiable information. When we think about why the privacy of the voters are vulnerable to attacks, we should consider internet infrastructure used. The wide usage of internet along with being targeted by the hacker community, there could be a large impact by the exploitation. Also, the voting machines could be from the third-party vendors. In this case, there must be an agreement with respect to the information shared. And, if in case the system is exploited, then who is responsible for the loss in the election process?
3. Uniqueness: Eligible voters should cast their vote only once (Nguyen, T. A. T., & Dang, T. K., 2013).
4. Accuracy: The votes that are recorded must be as intended by the voters. Also, it is important to ensure that the content of the vote cannot be modified (Nguyen, T. A. T., & Dang, T. K., 2013). A vote from an eligible voter must not be deleted or invalid votes cannot be added.
5. Fairness: It must not be possible for any electoral official to know the intermediate results of the election until it is publicly announced(Nguyen, T. A. T., & Dang, T. K., 2013). This could be considered as unauthorized access and might lead to political clashes.
6. Receipt-freeness: Receipt-freeness is one of the most fundamental factors to motivate the electronic voting system. By producing the receipt, the voter could prove that he/she voted for a particular candidate which might lead to unethical vote selling (Nguyen, T. A. T., & Dang, T. K., 2013). In order to avoid these political consequences, it is essential to have a receipt free process.
7. Uncoercibility: The decision to vote for a particular political party taken by the voter should not be influenced by an adversary (Nguyen, T. A. T., & Dang, T. K., 2013). It must be his/her own decision. Adversary must not force the voter either to cast a vote for their choice of political party or to disclose the vote that is casted.
8. Verifiability: It is the right of the voter to check if their vote is correctly counted or not (Nguyen, T. A. T., & Dang, T. K., 2013). This is challenging to achieve while considering receipt freeness requirement to be satisfied. But, there are other ways to address this issue. One such example is VerifiedVoting, a non-profit organization that ensures the vote’s verifiability (VerifiedVoting.org., 2019).
9. Security: Security involves both physical security of the devices used and also the network security of the electronic components used in the electoral process. Electronic components include the resources like servers and computer software.

There are various security attacks that the voting systems are susceptible to and they include:

1. Insider Programming attacks: These attacks are the result of poor programming, ineffective software engineering techniques used by the developers and the irregular patch management procedures. There is a possibility that the programmer could exploit the vulnerability in the software used and make the program run according to the commands he/she issues (David Jefferson, Aviel D. Rubin, Barbara Simons, & David Wagner, 2004). This attack provides the hacker to have full access to the system and thereby manipulate the votes. The hacker could delete the votes from eligible voters and hence affect the results.
2. Denial-of-Service attacks: In these attacks, the hackers do not focus on gaining unauthorized access to confidential resources, instead they focus on preventing the eligible voters from using the system. The hackers usually take up all the resources from the electoral web server which makes it difficult for the server to address the requests from eligible voters web browser. (David Jefferson, Aviel D. Rubin, Barbara Simons, & David Wagner, 2004). Confidentiality, integrity and availability are the three security requirements for any system to be secure and reliable. In this case, though the privacy of the voters are still protected, the availability of the voting system is affected.
3. Man-in-the-middle attacks: SSL is abbreviated as secure socket layer, a standard protocol for establishing a secure network between the web browser and the server. A hacker could act as a SSL gateway and receive all the votes from the voter’s web browser (David Jefferson, Aviel D. Rubin, Barbara Simons, & David Wagner, 2004). He/she could decrypt and compromise the voters’ privacy and then encrypt and send to the server. This type of attack is hard to identify.

Future work:

The US Defense Department’s Defense Advanced Research Projects Agency (DARPA) has awarded a $10 million contract to design and build a secure open source voting system. (DARPA is trying to build an unhackable open-source voting system, March 15 2019**)**. As per the voting system ethical requirements, it is said that the developing system will be verifiable and transparent. It allows the voters to verify the vote they have casted and thus does not violate the voters’ right. Also, the hardware and the software components used are open source and hence the researchers could evaluate the system built for vulnerabilities that could be exploited. However, online element might be discarded in the system being worked on by DARPA scientists.

With the constant effort and contribution from the researchers, technologists and electoral officials, it is possible to achieve the reliable and secure voting system. I think there are lot of ethical dilemmas involved in the online voting system due to the internet infrastructure that is widespread across the boundaries and used by millions. Ongoing projects that focus on voting systems that do not revert back to traditional paper ballots are motivated.

Conclusion:

With the widespread use of Internet, every traditional application is motivated to be developed as an e-commerce application and the voting system is one of that kind. However, with the fact that e-commerce applications are most prone to attacks that compromise their ethical goals, it is difficult to meet the exact expectations as that of traditional voting system. There are various entities like politics in this system as well as complexity involved, which makes the researchers more interested. The electoral officials should take into consideration all the possible intrusions and correct them to ensure the privacy of the voters before implementing for real time elections. The software components used must be designed in a way that the virus and malware attacks are difficult to perform. There should be a good balance in protecting the rights of the voters, enabling them to verify their votes and ensure their privacy is protected.

References:

Pieters, W. & Becker, M. J. (2005). Ethics of e-voting: an essay on requirements and values in Internet elections. Retrieved from https://www.academia.edu/2317557/Ethics\_of\_e-voting\_An\_essay\_on\_requirements\_and\_values\_in\_Internet\_elections

O’Keefe, K. and O’Brien, D. (2018). *Ethical Data and Information Management: Concepts, Tools, and Methods.* Kogan Page.

Robinson, D. G., & Halderman, J. A. (2012). Ethical issues in E-voting security analysis. (pp. 119-130). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-29889-9\_10

David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. 2004. Analyzing internet voting security. Commun. ACM 47, 10 (October 2004), 59-64. DOI: <https://doi-org.ezproxy2.library.drexel.edu/10.1145/1022594.1022624>

Nguyen, T. A. T., & Dang, T. K. (2013). Enhanced security in internet voting protocol using blind signature and dynamic ballots. *Electronic Commerce Research, 13*(3), 257-272. doi:10.1007/s10660-013-9120-5

VerifiedVoting.org. (2019) Retrieved from <https://www.verifiedvoting.org/about-vvo/>

DARPA is trying to build an unhackable open-source voting system. March 15 2019. MIT Technology Review