International Journal of Engineering & Technology, 8 (1.6) (2019) 34-39

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Challenges of Electronic Voting

Kalim Qureshi[1*] and Noha Abdallah[2]

[1]Kuwait University, Information Science Department,
[2]Kuwait University, Information Science Department
**Corresponding author Email: kalimuddinqureshi@gmail.com*

Abstract

In electron-voting system, different attacks and threats may be carried out depending on the operational environment in which the system is used. Voting systems can be easily exposed to attack from different serious threats of denial of service and a Man-in the-Middle attack. Cryptographic techniques like fingerprint sensor and digital signature scheme can be used in electronic voting. Combining two techniques like digital signature and blind signature or fingerprint may be the best solution for a secured electronic voting system. The purpose of this paper address the scope of electronic voting system, and examine the main security problems in electronic voting systems, particularly security threats related to electronic voting systems, the criteria of using electronic voting systems, and solutions to security threats.

Keywords: *Electronic Voting System, E-Voting Security, Cryptography, Threats, and Attacks*

1. Introduction

Electronic voting refers to voting through electronic channels. With the fast advancement of technology innovation, the use of computers has turned out to more helpful for ballots through using different means such as the Internet, telephone and a private computer network. Utilizing these means can offer many advantages in voting process electronically like, cost reduction, quickness of implementation, accessibility for disabled voters, and simplicity. However, electronic voting systems have limitations in security where voting process is vulnerable to serious attacks. Without appropriate security and successful control methodology, noxious performers may instantiate a scope of risk activities, with effects varying from a "denial of service" which sabotage electronic voting and stop election in the polling station and alter the results.
Barriers to electronic voting resides in "lack of common voting system standards, election laws, cost of certifying a voting system, security and reliability of electronic voting, access to Internet voting, skills, and need for security and election experts"[3].

1.1 Voting Environment

Electronic voting environment involves voters, authentication server to authenticate the Voters and grant Voting Tickets, voting servers to collect voting tickets from voters, and a "Ticket Counting Server (TCS)", with "Trusted Certificate Authority/Authorities (CA)" [1]. Authentic and secret communications between voters and servers are based on asymmetric key cryptosystems. Therefore, voters and servers do not share any secret.
Voting scheme has following common requirements [1-6]:

- Anonymity of Voters: Identities of voters must not be revealed to other voters and Voting Server. The authentication server cannot map any voting ticket to the corresponding voter's identity, unless the voter has double voted.
- Secrecy of Voting Tickets: The contents of a voting ticket should be secret and must be protected from unauthorized disclosure; while the contents are in the clear to Voting Servers.
- Authentication between Voters and AS: AS should know that the voters are legitimate for the given election and voters should know that AS is the authority which is issuing the voting tickets.
- Validation of Voting Tickets: Voting Server S is able to check the validity of voting tickets.
- Double Voting: It should not be possible for a voter to vote more than once1; if this occurs, then this can be detected and the identity of the voter revealed.

Technical Components of Electronic Voting System are define in [1, 2, 6]

- Elections Calling
- Voters & Candidates Registration
- Polling list Preparation
- Votes Counting
- Auditing, Reviewing, and Follow-up

Criteria for E-Voting System Design is define in [1, 5, 7]

- Authentication: Only authorized voters can vote

Copyright © 2019 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

- Uniqueness: only one vote for each voter
- Accuracy: by recording votes errorless
- Integrity: not modifying votes without detection.
- Verifiability: that votes are correctly counted for in the final stage
- Auditability: a reliable and authentic election records
- Secrecy: Only voters know how they vote
- Convenience: Voters can vote with "minimal equipment and skills"
- Verifiability: Systems should be testable against essential criteria
- Transparency: Voters must understand voting process
- Cost-effectiveness: Systems should be affordable and efficient
- Reliability: Systems should work robustly

Technologies for Electronic Voting System Security is define in [3, 4, 6]

- Cryptography: like digital signatures, blind signatures, Trusted Third Parties, digital certificates, etc.
- Antiviral software
- Firewalls
- Biometrics (e.g. fingerprint sensor)
- Smart cards

2. Other researcher works

Researchers' efforts are exerted to find ways of tailoring electronic voting technologies that meet the needs of legal regulations, technical advances, and the dynamics of social and psychological contexts. To that end, new application areas of voting technologies arise, such as proxy voting, mobile voting, or spontaneous and secure decision-making voting in small communities. These new directions, however, also pose new challenges like identifying and defining usability and practical feasibility.

A number of papers were selected for this issue, each of which makes a significant contribution to the debate on new directions in electronic voting. The work by Abba et al. [1] addresses the question of the extent to which privacy of an election is at risk due to unanimous voting. The author applies his theoretical investigation to a real-world election in USA. In 2016, some states in USA called for recounts for general elections due to suspicions in voting systems security. The paper examined the "current and future risks and perils to the security of elections" [1]. With these citizens are willing to vote, vulnerabilities can be significantly reduced only if appropriate and adequate measures are taken and implemented in every election, at all levels [1]. The work of from Craig et al. & Pan et al. [3, 5], connects to the work of [1]. by discussing security problems for e-voting by exploring E-voting systems with their empirical studies. In [5], surveyed and deployed an E-voting system for Victoria State in Australia using open source software, while [3] built a new system, based on previous works, referred to as "Enhanced Name and vote separated E-voting system". "Enhanced Name and vote" used a protocol and a "watchdog hardware device" to ensure confidentiality and accuracy. The "watchdog device" records all voting activities during the election to prevent any disputes or any other malicious behaviors [3, 5]. The messaging protocol is based on XML. Thereby the authors build the foundation for defining an adequate trade-off between secrecy of the votes and enforcing the public nature of the elections.

In Abo Samra et al., and Nisha et al. [4, 2] addressed new approach for online voting system and mitigate risks with anti-phishing implementation like Visual Cryptography Technique. Visual Cryptography technique can find out whether voter is in phishing site or original site easily. This can improve further voting process especially for abroad, old, and disables voters. Like any secured system, design of electronic voting requires great care and evaluation of its environment. Analysis from a "system perspective" has provided valuable insight into consideration during the design and evaluation phases, and then there should be every reason to suppose that cryptographic voter verifiable voting schemes could provide high assurance elections. A threat model for E-voting test and risk mitigation can measure more like a simulation model in order to have a uniform, confidential, secure, and verifiable E-voting system.

To conclude, the papers included in this special issue contribute by highlighting the challenges of electronic voting from a number of different perspectives. They also provide an overview of the challenges, risks, and barriers with proposed solutions (theoretically and empirically) in the domain of voting technology. Table (1) summaries the related works for this research paper.

3. Challenges for e-voting system security

Studies revealed four elements that are acting as the source of threats and attacks which can threaten the integrity of elections and undermine confidence in democratic processes as well. For example, malfunction of electronic equipment, errors in software programming, delete of ballots or manipulated by privileged actors, and undermining of voters’ privacy.

The technical areas that pose problems in electronic voting security are [6]:

- Denial of service attacks where hackers overload a system with requests of information. This can prevent voters from casting their ballot.
- Viruses/malicious software which corrupt voting software installed on voter's equipment, therefore affect casting process.
- Servers' Hackers, which can affect the integrity of the voting counts (e.g. breaking the computer systems to alter, copy or damage data records and software).
- System capacity Limitations which should cope with heavy demands during voting period.

Voting protocols are important for voters' privacy. It is a process of using authentication means to prevent non-eligible voters from voting, and to prevent eligible voters from re-voting. Likewise results must keep secret to the end of election in order not to affect people who have not yet voted. Other essential voting protocols are verifiability which provides voters with the "ability to verify that their votes have been treated correctly"[7]. Table (2) show voters' IPO (input/process/output) for voters' privacy and authentication.

4. Attacks on electronic voting & solutions

Even though electronic voting systems have a great number of advantages like cost reduction, flexibility, and convenience, several problems can associate democratic voting process electronically. Table (3) & Table (4) present attacks and security threats on Electronic Voting and their effects [6, 9, 10].

Table 1: Summaries of the recent research works

Empirical studies conducted on E-voting security:		
Paper Reference No. and Year	Finding	Remarks
[5], 2016 [3], 2014	Both papers conducted a survey and proposed a deployment for E-voting. For [5] used open source for Victoria State-Australia voting system, while [3] presented improved E-voting based on previous works with a new protocol design and a watchdog hardware device to ensure confidentiality and accuracy.	The findings of both studies deployed a new E-voting system to ensure voter's confidentiality, candidate privacy, and voting accuracy, using encryption and shuffling of the candidates' names on the ballot for additional protection to secure the privacy and fairness of the election.
Cryptography proposal models for E-voting:		
[4], 2016 [2], 2017	Both studies focus on the problems of security on online voting system, and proposed a new approach for online voting system with anti-phishing implementation like Visual Cryptography Technique. Also how to mitigate risks.	The findings of both studies emphasized on using proposed approach to improve voting process and especially that some citizens are living abroad and others are disabled or old. Electronic voting should be uniform, confidential, secure and verifiable. It appears that security features are only one premise underlying a system's acceptance among the electorate. There exist a few cryptographic schemes which fulfill a wide range of e-voting requirements.
Descriptive studies that focuses on vulnerabilities and E-voting security:		
[1], 2017	The paper is descriptive for E-voting system phases and the importance of security in E-voting systems. The paper examines some states in USA where calls for recounts in the 2016 general elections were requested due to suspicions in voting systems security. It analyzed the risks and perils to the security of elections, and vulnerabilities that will be confronted in the future.	The paper presented recommendations about how to lessen risks associated with E-voting, and concluded that vulnerabilities can be significantly reduced if appropriate and adequate measures are taken and implemented at all levels of election.

5. Elections and voting equipment security plan

A security plan for voting equipment's can define measures and standards in each of the following aspect [8]:
(a) The storage of election equipment hardware and software and related election materials, including maintaining the following:

- A list of all personnel with keys and access to the election equipment storage area;
- An access log including sign in and out times and dates of all personnel given access to the storage area;
- A list of all equipment by serial number and quantity; and
- An inventory record of each piece of voting equipment, including serial number, a history of repairs, replacements, and upgrades, Log details, etc.

(b) The storage and tracking of paper ballots, and a record of all security seal numbers used to seal ballot containers and tabulators [8].
(c) The processing and storage of voter registration and voting records in the clerk's office [7, 8].
(d) "Password administrator" to issue passwords, maintains a master list of all passwords issued, and reissues all passwords on a periodic basis [8].
(e) A checklist for precinct election officers to follow for opening and closing the precincts on Election Day, including:

- A procedure to "count and verify all paper and provisional ballots, and election supplies prior to the opening of the polls" [8];
- A procedure to validate the number of voter activation devices after the polls have closed and secure the devices for transport back to the county clerk's office; and
- A procedure for securing and accounting for all voting equipment after the closing of the polls;

(f) Securing and storing the voting equipment after "Election Day and in between elections and maintenance of election materials for the period required pursuant to the law" [8]. Table 5 presents solutions to security problems related to E-voting system.

Table 2: Input/Process/Output (IPO) related to voters [8]

Input	Process	Output
Voter ID	Check if on electoral roll Check if already voted Retrieve candidates from endorsed candidates file	"Not allowed to vote" "Already voted" List of endorsed candidates
Vote, candidate name	Update voter's record with 'voted flag = 1\Retrieve candidates record Increment count in candidates record and rewrite.	Update voter's record Updated candidates record 'Thank you for voting'
Candidates file	Read in each candidates record to an array of records Sort these records into descending order of votes	Report of results showing candidate name, number of votes.

6. A simple proposal for e-voting

The concern for voter privacy is still a challenge, even for secure systems. Most audit techniques involve going through logs and determining who performed which tasks. Therefore, designing is important for a secured system to allow for anonymous votes. For example when a server receives a vote, it stores it securely until the time when all votes are counted. Also, votes are encrypted with a public key of authorized entity and decrypted with the corresponding private key.

Finger print is a simple technique can be proposed for the security of voters and votes. This technique is fingerprint sensor. Fingerprint sensor is a practical way for Electronic voting process and economical. The process consists of scanning voter's thumb to provide high performance and security to the voting counter via displaying the data-base of the voter.

Table 3: important attacks on electronic voting system

	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (With access to network traffic)	Internet Provider (with access to network traffic)	OS Developer	Voting Device Developer
Vote multiple times using forged smartcard	●	●	●			
Access administrative functions or close polling station	●	●			●	●
Modify system configuration		●			●	●
Modify ballot definition (e.g., party affiliation)		●	●	●	●	●
Cause votes to be miscounted by tampering with configuration		●	●	●	●	●
Impersonate legitimate voting machine to tallying authority		●	●	●	●	●
Create, delete and modify votes		●	●	●	●	●
Link voters with their votes		●	●	●	●	●
Tamper with audit logs		●	●	●	●	●
Delay the start of an election		●	●	●	●	●
Insert backdoors into code					●	●

As the voter pressed thumb on the finger print sensor, the sensor scans the image of the fingerprint and its unique pattern then generates a digital signal in ones and zeros. The digital output is stored against voter's database, whom the fingerprint is related, at a local center.

During the election, and as the thumb is pressed, checked, and match with the record data base with user figure print then and then only the overall system allows to voter to vote his/her respective party at that same instant screen (like LCD) displays the name of party you vote for. If the fingerprint is not matched then system displays "Data is not found" or "rejected" in case the voter tries to vote for a second time. Figure 1 illustrate system sequence diagram of e-voting.

Table 4: security threats to internet voting systems [9-13]

Threat Type	Meaning & Effect
Denial of Service Attacks (DoS)	DoS when an attacker makes the server unavailable for use. This prevents voters from accessing election web. There are four patterns of DoS attacks: - flood the election web server with a series of messages to "obstruct the network and prevent voters from accessing election web". - "disconnect connections between two computers" to prevent access to the election web. - make the election web "unreachable to a particular system or a legal user". - prevent "a specific person" from accessing the election web. As a result of such DoS attacks, serious security problems can lead to influence the justice of the election.
Virus Infestation and Malicious Software	Malicious code is known as malware that "threats using the Internet voting system". This software damages computer systems and is "distributed through Trojan horses, viruses and worms". The two malicious codes for the Internet voting systems are: - Plant malicious software into the election web server by "developers to destroy the vote data". - "Distribution of malicious software into voters' computers", thus affecting the election process. Such malicious software may be difficult to detect, because some anti-virus programs cannot detect new viruses; therefore, affect the voting process without the voters' knowledge and changing the voter's data or dropping votes.
Spoofing Attacks	Spoofing attacks is deceiving voters that they are communicating with the real election web server (Man-in-the, Middle) by redirecting the voter to fake election web server. Therefore, tamper with votes in favor of a particular preferred candidate and also invade voters' privacy through mining the personal information.
Phishing Attacks	Phishing attacks start with an e-mail or an advertisement on the world wide web to tempt the user into clicking a link. The link leads to a website where the attack takes place and asking the user to enter a password or disclose credit card number, or attack the user's browser directly to spy on the user's future online activities. With e-voting, an attack, a voter visits a copy of the E-voting website which has been "created by attackers". On the site, the

	voter is asked to enter identification code and may even be taken through a bogus voting process where vote cast would never find the way into the official ballot box.

Table 5: Solutions of Security Problems [9, 10]

Solutions	Meaning
The Use of Open-Source Software	Open-source software is a source code released to the public to be tailored based on their needs, e.g. Linux. An open-source code enables developers to discover errors and modifications in the voting results. However, there is no guarantee that the code source, which has been inspected, "is the same code source used in electronic voting systems. It may also, be exploited by hackers to change the software's code source".
Using Voter Verifiable Audit Trails (VVAT), also known as a Voter Verified Paper Audit Trail (VVPAT)	The lack of a VVAT (known as VVPAT) is a fundamental security problem of using electronic voting systems. The use of VVPAT can "preserve electors' votes as a backup paper system in case of exposure to attacks" such as DoS attack or recover from modifications in the voting results.
Using Layer (SSL) Protocol	Secure Socket Layer (SSL) protocol may mitigate the threat and prevent a third party from manipulating the voting results. The key feature of using the SSL Protocol is to "distinguish between a SSL election web and a non-SSL election web". However, SSL protocol is vulnerable to hacking through the "decrypting of transmitted data". Voters, beside cryptographic methods like SSL, are responsible to raise their awareness when browsing a legal election web address and should know the difference between a real election web server and a malicious one from "web address (https – Hypertext Transfer Protocol)".
Using a digital signature scheme	Digital signature verifies that input data comes from an authorized voter. As a result, prevents unauthorized users/attackers/ illegitimate voters, from accessing the election data centre. A digital signature can prove voter's eligibility, but cannot keep voter's vote confidential and voter's privacy over the internet. For this, blind signature with digital is effective solution. A blind signature "conceals the content of a vote while verifying that the voter is eligible".

7. Conclusion

Voting systems are vulnerable to attacks like denial of service and a Man-in-the-Middle attack, and phishing. Also, electronic voting hardware and software can have flaws that affect the security process of any electronic system. For the security of E-voting, cryptographic techniques, like fingerprint and digital signature, are methods that can improve security environment, especially when combining two and more cryptographic technique, in addition to using a Voter Verifiable Audit Trail (VVAT).

Security issues in electronic voting reside in two main areas, the technical security and the procedural. Even though there are limitations with the technical security, enhancing the level of procedural side of it is important. Saying this, this research has concluded that threats can be as a result of:

- Insufficient and lack of detailed procedures to control specific activities prior and during the election
- Unclear procedures to control government officials' tasks with undefined responsibilities.
- Inadequate measures of procedural security that can cover all aspects of the electoral process.
- Lack of compliance to standards and requirements.
- Design problems and inadequate staff training to use the system
- Ignoring testing plans, and auditing

For future scope, empirical studies using other cryptographic techniques can improve the voting process over internet. Biometric advances can be implemented in this regards especially for illiterate and disability people. Finally, to make the voting process more secure, reliable and confidential, electronic voting systems must meet the current generation security requirements.

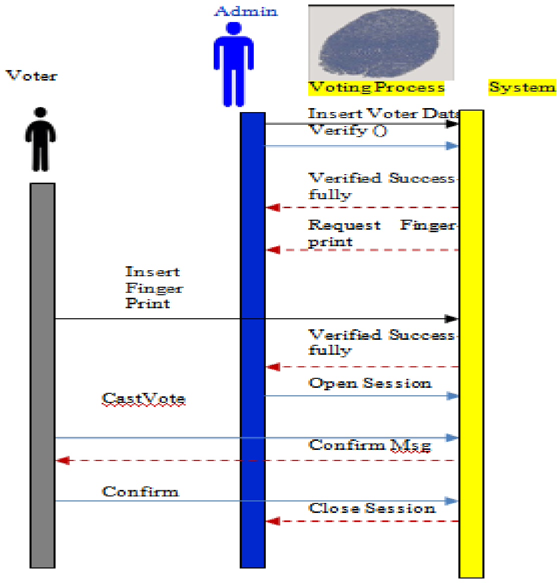

Figure 1: E-voting System Sequence Diagram

References

[1] Abdullahi Lawal Abba , Mohammad Awad, Zakaria Al-Qudah, and Abdul Halim Jallad, "Security Analysis of Voting Systems", IEEE International conference on electrical and computing techniques and applications, 2017.

[2] Kareem M. Abosamra, Ahmed A. Abdelhafez, Ghazy M.R. Assassa, Monan F.M. Mursi, "Practical, Secure, and Auditable e-voting system", Journal of Information Security and Applications, Vol. 36, pp. 69-89, Elsevier, 2017.

[3] Hiaijun Pan, Edwin Hou and Nirwan Ansari, "Enhanced name and vote separated E-voting: an E-voting system that ensures voter confidentiality and candidate privacy", Security and communication networks, vol. 7, pp.2335-2344, Wiley, 2014.

[4] S.Nisha, Neela Madheswari, "Prevention of Phishing Attacks in Voting System using Visual Cryptography", International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), pp. 3-35, 2016

[5] Craig Burton, Chris Culname, Steve Schneider, "vvote: Verifiable Electronic Voting in Practice", Security Smorgasbord, IEE computer and reliability societies, 2016

[6] Abdelwahab alsammak, Alaa abdelrahman, Tarek elshaistawy and aboubakr Elewa, “Cahllenges of Electronic Voting- A Survey”, ACSU Advances in Computer Science: An International Journal, Vol.4, issue 6, B0. 18, pp. 98-108,November 2015.

[7] Pankaj Kumar Malviya, “E-Voting System Using Cloud in Indian Scenario”, International Journal of Engineering Science & Advanced Technology, Vol. 3, Issue 3, pp-171-176, 2014.

[8] Modelling Tools - IPO diagrams URL: https://sdd-hsc-online.wikispaces.com/Modelling+Tools+-+IPO+diagrams

[9] Nwogu Emeka Reginald, “Mobile, Secure E-Voting Architecture for the Nigerian Electoral System”, IOSR Journal of Computer Engineering, Vol. 17, Issue 2, pp. 27-36, 2015.

[10] M. Nandha Kishore, A. Sridhar, S. Divakara,, “Advanced Security Strategy in Smart E-Voting System”, SSRG International Journal of Computer Science and Engineering, vol. 2, issue 6, pp.54-60. 2015.

[11] Rohan Patel, Vaibhav Ghorpade, Viny Jain and Mani Kambli, “Fingerprint Based e-voting System using Aadhar Database”, International Journal for Research in Emerging Science and Technology, Vol. 2, Issue 3, pp. 86-90, 2015.

[12] Olayemi M, Olaniyi, Taiha A. Foloruni, “Design of Secture Electronics Voting System using Finger Biometrics and Crypto-watermarking Approach”, I.J. Information Engineering and Electronics Business, Vol. 5, Issue 9, pp. 9-17, 2016.

[13] atchaya arivalagam, nage nikitha peddi, wajdi bazuhair, elt, “study of wireless security attacks on medical devices”, international journal of multi-disciplinary in cryptology and information security, vol.6 no. 6, November-December, 2017, pp. 2320-2610.