ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Challenges of Electronic Voting - A Survey

Abdelwahab AlSammak[1], Alaa AbdElRahman, Tarek ElShishtawy[2] and AbouBakr Elewa[3]

[1] Faculty of Engineering (Shoubra) - Benha University
[2] Faculty of Computer and Information - Benha University

[3] Ministry of Foreign Affairs
abdelwahab.asammak@feng.bu.edu.eg, alaaomarster@gmail.com ,t.shishtawy@ictp.edu.eg, elewabakr@hotmail.com
http://www.feng.bu.edu.eg/

Abstract

Electronic Voting (e-Voting) is the most important application in e-Government and e-Democracy. Thanks to the rapid growth in the use of computers and advances in cryptography, it is a serious push for e-Voting because many people already have access to the Internet. e-Voting can be the fastest, cheapest, and most effective way to administer the election, count the votes, and report the results. The main purpose of this paper is to highlight the major challenges facing e-Voting systems, introduce different ideas to face those challenge from different countries, and to explore the advantages and disadvantages of those ideas. Each of the challenges presented in this paper must be taken into account in crafting a legal framework for e-Voting to prevent harm before balloting is concluded.

Keywords: *Electronic Voting, e-Voting, e-Voting Requirements, e-Voting Challenges, Anonymity, Privacy.*

1. Introduction

1.1 Historical Background

The birth of democracy was in Athens in the sixth century B.C. where the first form of electoral laws was introduced [1]. Since that time, electoral systems have been designed and developed according to the characteristics of the countries in democratic governments around the world. Voting systems have evolved in response to the problems and the needs of political systems [2].
In many countries, interest in e-Voting is growing very rapidly. The number of e-Voting experiments taking place is also growing with different approaches and motivations of each country. By closely studying these experiences, it is possible to learn new and interesting lessons, lead to different schemes, and create a valid e-Voting system.

E-Voting machines were in use in the Netherlands for 20 years, with nearly the whole population vote using one of the DRE (Direct Recording Equipment/Electronic) voting systems available to vote. The introduction of this technology in the 1980s was not preceded by a public debate. In 2006, 90% of all votes in the Netherlands were expressed on the computer [3].

The birth of democracy was in Athens in the sixth century B.C. where the first form of electoral laws was introduced [1]. Since that time, electoral systems have been designed and developed according to the characteristics of the countries in democratic governments around the world. Voting systems have evolved in response to the problems and the needs of political systems [2].In many countries, interest in e-Voting is growing very rapidly. The number of e-Voting experiments taking place is also growing with different approaches and motivations of each country. By closely studying these experiences, it is possible to learn new and interesting lessons, lead to different schemes, and create a valid e-Voting system

E-Voting machines were in use in the Netherlands for 20 years, with nearly the whole population vote using one of the DRE (Direct Recording Equipment/Electronic) voting systems available to vote. The introduction of this technology in the 1980s was not preceded by a public debate. In 2006, 90% of all votes in the Netherlands were expressed on the computer [3].

The idea of e-Voting was introduced in Estonia I 2001. Their vision was to introduce Vote-over-Internet (VoI) in uncontrolled environments. Although at first they thought VoI could be used in the 2002 elections, they had to wait until 2005 to be a real option VoI in local elections. The first objective of VOI is to increase the participation maintaining voter interest in voting and increasing the interest of the younger generation. The other objective is

to stay in touch with modern Information and Communication Technology (ICT) and facilitate voting [4].

In 2002, the first e-Voting was conducted in Japan. Since then, ten local governments have conducted a total of twenty cases of e-Voting. In Japan, after “e-Japan Strategy", which aims to build an e-Government, was released in January 2001; many e orts of an e-Government and e-Democracy have been attempted. E-Voting can be seen in this trend [5]. In Korea, the participation rate is declining, a fact lead some to find a way to increase the participation rate. But an increase in the participation rate does not necessarily promote the quality of the representation itself. Due to the disproportionate representation in society, it can also over-represent the group that has been over-represented while an under-represented group becomes more under-represented. Therefore, improving the quantitative representation only make sense if the qualitative representation is made at the same time [6].

1.2 **Definitions**

Election An election is a process to obtain accurate data, representing a set of participants' responses to a question [7].

Voting, Voting means the fact to freely express choices between alternatives known to the public, e.g. candidates [8]. Voting is the most fundamental act of our democracy. Votes are mandatory for expressing people's will, which must be both secret and restricted to only one per citizen. It should be secure enough, easy to register, easy to vote, and easy to count the votes. Voting systems should comply with the principles of non-discrimination and democratic elections [9].

Vote, A vote is that physically represents the response of a participant in a particular issue. A vote is a selection, usually from a predetermined set of responses called candidates. Sometimes a vote includes a selection, which is not a member of the predetermined list, and is called writing -in stations [7]. The vote is the most powerful tool to express the content and citizen control over government agencies. The vote should not be understood as a mechanical process, but as having a capacity to create its own, because it provides unification of the people. Although the act of voting is considered a personal right, the process engages the development of the nation as a whole. The choices of procedures and tools in place to support the “unification" are of vital importance because they must respect the creative capacity of the unification process, without introducing disparities [9].

Ballot, One or more votes are grouped in a structure called a ballot. Each question in an election is called a race, so each race has a set of candidates potentially receive the votes of electors [7].

E-Voting, e-Voting is a term encompassing several types of voting, includes both electronic means of casting a vote and electronic means of counting votes. E-Voting technology can include punched cards, optical scan voting systems, and specialized voting kiosks. It can also involve transmission of ballots and votes via telephone, private computer network, or the Internet [10]. E-Voting types fall into two major categories:

- On-site e-Voting (supervised by representatives of governmental with e-Voting machines at the polling station)

- Remote e-Voting (not physically supervised like voting using computer via the internet, using mobile phones via SMS, or at public kiosks).

Electronic elections are conducted either using DRE machines or over the Internet. Although DREs have benefits such as speedy results, accuracy, reduction in manpower and paperwork, they are vulnerable to sabotage and equipment malfunction. Further, if a malfunction is detected, there seems no way to conduct a recount and the only remedy is a recast of ballots. Internet voting provides ease of access and eliminates absentee ballots, but is surrounded by many more security concerns than the DRE systems. Figure 1 illustrates the flowchart of classical voting, on-site e-Voting, and remote e-Voting, in the same time fig 2, illustrate how I-voter can vote using any device connected to the internet.

Technology is very promising to serve as a mean to cope with the crisis of participation and confidence that democracy faces todays [11, 12]. For example, it can be used to make democracy more accessible to citizen as e-Voting can provide great opportunities for improvement of certain groups access to the electoral process. The following groups are eligible [2]:

- Visually impaired citizens can use a headset connected to DRE or the PC if Internet voting is used. - Minorities can access e-Voting systems in their preferred language.

- Citizens living and working abroad can vote online from their own homes. Citizens who cannot attend at a polling station to cast their votes can vote Online from their own homes.

2. Requirements of e-Voting

Requirements of traditional voting (paper ballot) are also valid for e-Voting like complying with the principles of non-discrimination and democratic elections. Any voting system must meet the following requirements [13, 14, 15].

Universality, all voters have the right and ability to vote using the system

Authenticity, only eligible voters can participate.

Uniqueness, No voter should be able to vote more than once.

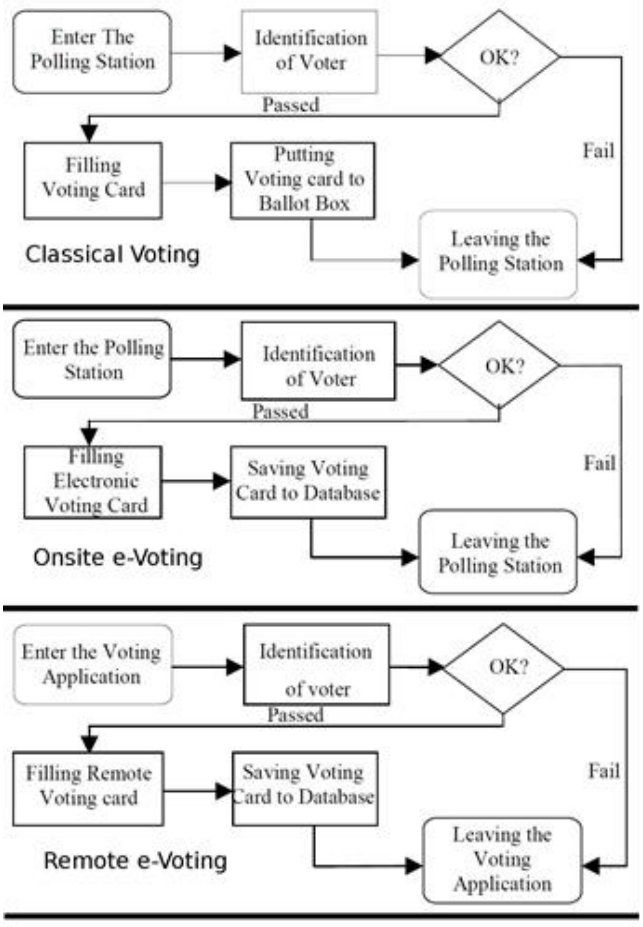

Fig. 1. Classic voting vs. On-site e-Voting vs. Remote e-Voting

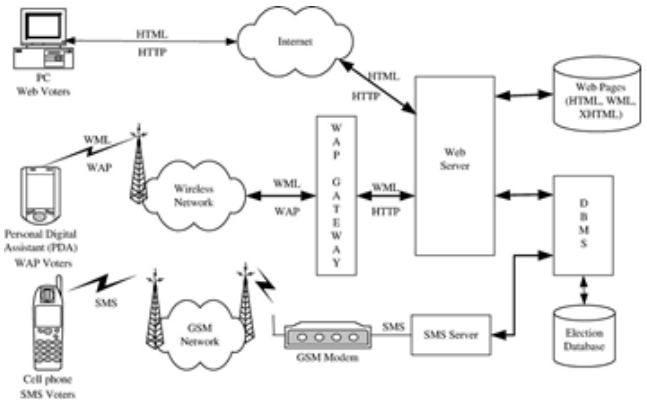

Fig. 2. An example remote e-Voting system

Reliability, the system should function without compromising votes, even if system failure occurs

Accuracy, the votes are properly recorded.

Integrity, Votes cannot be edited or deleted.

Flexibility, the system should be usable by different types of voters (support multilingual voting ballots, accommodate disabilities by audio or visual features, support different input methods, etc.).

Convenience, Electoral systems should not require additional skills to be usable without unreasonable need for equipment.

Transparency, Voters should be able to understand the overall system.

Secrecy, Votes should be secret and a voter must not have a record of voting choices.

Anonymity, Each voter has the right to cast his vote secretly, and no one should be able to relate a voter to his/her vote.

Freedom/Uncoercibility, The citizen must be able to vote without being forced by the government to vote for a particular candidate.

Audit/Accountability, The system has the ability to verify that votes are properly counted.

Verifiability, the system must be tested by election officials.

Cost, the system should not be too expensive.

A voting protocol is said to respect privacy when an intruder cannot detect if arbitrary honest voters VA and VB swap their votes. In general, this means that the intruder cannot know anything about how VA (or VB) voted. This can be expressed as follows [16, 17]:

$$S\,[VA\ \{a/v\} |\ VB\ \{b/v\}] \approx S\,[VA\ \{b/v\} |\ VB\ \{a/v\}]$$

Even if the result of the election is necessarily revealed, the definition above is still robust [18].

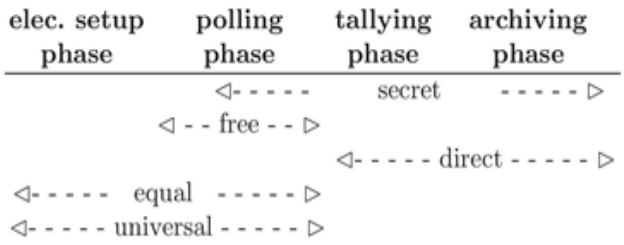

Fig. 3. Election Phases and requirements

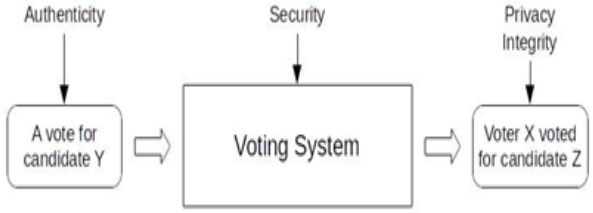

Fig. 4. Requirements of Voting

Unfortunately, some satisfying some requirements contradicts with satisfying others. This results in some challenges. In the following section, challenges of e-Voting systems are introduced. Voting in Egypt is like any other country; most countries still using the traditional voting technique to elect the government, but the Egyptian government now thinking about electronic rather than conventional Vote, to avoid the problems they are facing. Where there are many problems in the conventional voting system used in Egypt, like:

1. Relation between the government and the people usually suffers from lack or trust.

2. Sometimes, government coerces and carries on the voters to vote for a particular candidate, and eliminate them from voting freely.

3. Some candidates trying to win by buy the votes from the voters.

4. Government can cheat by substitute the original ballot by derivative ones.

Therefore, there must be another way to solve these problems or reduce it as much as possible, and give the voters the confidence to believe in the system. Consequently, new technologies must be used to improve the election process by building new systems that are more convenient to people [13].

3. Challenges of e-Voting

It is important to control and to observe different stages of the election process. It is necessary to be able to guarantee the well-functioning of the system before the start of the election period, during the voting period and afterwards. This means that there must be a focus on certification processes before the processing of the data actually begins as well as on proper mechanisms for post-auditing of the elections [19, 20].

3.1 Legal Challenges the fact that municipalities are legally obliged to keep a registry of eligible voters is certainly also favorable for any e-Voting system [21]. Law and consequently the constitutional law de ne clear and strict regulations for voting and instruments used. To use the computer-aided communication in these fields, used techniques must satisfy the relevant legal requirements [22]. Any attempt to introduce e-Voting, i.e. a voting process, which enables voters to cast a secure and secret ballot over the Internet or an Intranet, will have to address a series of complex constitutional and legal issues. Our paper refers to these democracy-oriented legal and constitutional requirements, which every electronic voting system has to comply with [11]. On the other hand, law can provide legal protection to e-Voting systems. Attacks against mission-critical systems in countries like the United States and the United Kingdom are treated as criminal cases for which the perpetrators must be prosecuted. The act of hackers/crackers unauthorized access to a computer system can be compared to someone breaking into a home as a way to check if it is secure [23, 24].

Voter Identification; Identification and authentication of the voter when e-Voting is used at a polling station, the voter identification process may remain the same, but it can also change if an electronic register of voters used. In this case, arrangements should be put in place to ensure that the identity of the voter cannot be linked to his/her voice. If biometric features have been used for the registration process, these features can be used for voter authentication. Vote home Internet is different and an electronic remote identification system must be developed. Voters could authenticate with an electronic identity card having voter credentials or, if such a system exists, authenticate using a combination of user name and password with a control issue (e.g., date of birth). It is important to realize that without a physical token, authentication of the voter is less reliable and it is much easier to sell his vote in disclosing the user name and password to a third party. It should be noted that when voters must make their own user name and/or password (for example, when registering to vote), they may forget or misplace the username and/or password. Thus, a system must be established to provide a username and/or password in the short term while at the same time as the voter can vote only once [2, 25, 26].

Verifiability; is a central institution of modern e-Voting systems. Intuitively, verifiability means that voters can verify that their votes were counted and the election published result is correct, even if the voting machines/authorities (partially) unreliable [27].

Maintaining Anonymity to preserve the secrecy of the vote as one of the main principles of democratic elections, it is important that at some point in the voting process, the link between the identity of the voter and the vote itself is divided (which is also known as unlink ability). This should preferably be done immediately after the voter has cast his/her vote. Since the vote and the voter should not be linked, it is important to establish an administrative procedure that has access to register to vote and voter lists (preferably managed by different authorities), when and under what circumstances they will access, how long records exist, and how and by whom they will be deleted. In case of reversible vote, specific technical solutions must be implemented [29, 30,31].

3.2 Social & Cultural Challenges

E-Voting was introduced in Belgium in 1994. Ironically, no action had been taken to determine the opinion of facing this original method of voting constituents. In [32], the social and empirical dimensions of the legitimacy of this new method through several empirical indicators used in an investigation on the occasion of May18, 2003 federal election: (A) It was difficult for voters to vote for a computer; (B) the extent to which they trust to vote on a computer; (C) if they have a philosophical/social opposition to a vote on a computer [32].

The result of this provision inserted in the Belgian electoral law by the Act of 11 April 1994 was the introduction of a voting system of the computer in a growing number of municipalities for all elections in Belgium since the 19942 system used in Belgium is separate from Internet voting and voting by computer network. Voters go to the polling station where they are asked to vote on the computer. The objective of the system is to make the voting and vote counting easier and faster [32].

Paradoxically, this new method of voting had not yet been evaluated in depth. In particular, no action had been taken to determine the opinion of facing this original method of voting constituents. For this reason, during federal elections of 18 May 2003, Belgium, the authors conducted a large survey of voters leaving the polls to determine the views of the Belgians on e-Voting immediately after using this new technique of vote. Two main issues were considered: (a) the extent to which e-Voting, as used in Belgium is considered easy or di cult to use, and

(b) If e-Voting is socially accepted or rejected by voters who use? For example, it should be noted that 20.37% of voters without education considers that e-Voting is `di cult' or `very di cult'. There is a digital divide to consider, even if it is not striking [32].

In December 2006, the federal and regional governments have asked a consortium of seven Belgian universities to present a study on the legal technical, Organizational, socio-political and a range of voting systems. In addition, special attention should be given to the accessibility and usability of the system for people with disabilities [33].

A research team of the Universit libre de Bruxelles (ULB) verified the legitimacy of e-Voting in 2003; the main conclusion was that 88% has a favorable attitude towards the system, while 8.5% unfavorable (the rest 3.5% had no opinion or did not answer).

More detailed results are as follows: 95% of voters easily find the system very easy to use and 85% have no problem in principle with e-Voting, and 89% are fully con dent or somewhat con dent in the e-Voting system [33].

A majority of voters who had confidence in e-Voting also expressed his confidence in the ballot, but more moderately. On the other hand, those who dis-trusted the new method are those who have contributed most ballots. While the Belgian e-Voting system is not as vulnerable as DRE used in countries such as the United States, the Netherlands, and France. Indeed, this computer can overwrite a vote and subsequent verification of magnetic stripe cards will not reveal such an attack. In addition, the central production and distribution disk requires a complex chain of custody in which the focus should be trusted (eg, how can someone be sure that the software is released later

the same as the software running on each computer station?) [33].

Furthermore, some irregularities have been reported, for example, with respect to the management of passwords to activate devices. Voting machines are themselves \stupid" machines that do not store the ballots, but it is not in-conceivable that the material of such a machine can be changed to attack the privacy and/or the integrity of the vote. These machines can also be vulnerable to side channel attacks, for example, based on the electromagnetic analysis. As these machines are quite large and not useful for any other purpose, it is unlikely that they are stored in a place high physical security. The paper-based system is not without flaws, namely: the authors were informed (off the record) that frauds are known in which votes for specific candidates are added during the counting process. It is also very easy to spoil a ballot by an additional mark on it [33].
Voters were able to vote by electronic ballot box instead of throwing a bulletin plain paper in a traditional urn. The electronic ballot box was designed as a computer with a touch screen, like a terminal Mini Bank. Ballots submitted electronically were counted as regular ballots in the election. Experience Oppdal was more comprehensive than the rest. Oppdal municipality has nearly 5,000 voters, and electronic option was available in all seven areas of the town vote [4]. 91% of the electorate voted electronically to the election Svalbard. In the municipality of Bykle 53% opted for the method of e-Voting. In Oppdal 34% of the electorate voted electronically. In the district a voting Larvik, stre Halsen, 18% opted for electronically [4].

Family Voting Concerning the problem of “family voting" and similar possible in influences on the individual voters decision, which represent a major criticism of the use of internet voting, it was brought up that postal voting suffers theoretically from the same problem and that there exist means to guarantee the voters expression of free will (e.g. by introducing the possibility to recast the vote when it was cast via internet).
Vote Buying Any person who purchases or offers to purchase a vote of any elector at an election by the payment of money or the promise to pay the same at any future time, or by donation intoxicating liquor or anything else of value, are considered guilty of an offence. Every voter in an election that takes or receives money or other thing of value, provided that the same shall be paid at any time in the future in exchange for voting as an elector for a particular candidate, or promise to vote for a particular candidate, is guilty of an offence [34]. Coercion and vote buying: These risks are significant as it is impossible to prevent situations in which the voter casts a vote under pressure, or proves to a third party whom she/he has voted for [33]. Receipt-freeness are necessary to prevents vote selling/buying, ensuring that voters are not used as a proxy to cast votes [8, 35.36].

3.3 Technical Challenges

Design Flaws; An important decision when defining a strategy for e-Voting is whether to use open-source or proprietary software. This is particularly relevant to the question of trust. Many companies use proprietary e-Voting software, which has the disadvantage that in most cases, the rights holder is not the source code available to the general public (or makes available partially or temporarily) [2, 37].
In [35], security analysis of the source code of Diebold AccuVote-TS 4.3.1 has been introduced. It is one of the first electronic machine paperless voting systems used in a large market share. It is based on Windows CE and is developed in C++. The analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. Several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor development process software were identified. Without any insider privileges, can make unlimited votes without being detected by mechanisms in the terminal software to vote. In addition, Even the most serious of our outsider attacks could have been discovered and executed without access to the source code. Faced with these attacks, the usual worries about insider threats are not the only concerns; foreigners can do damage. The insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate the privacy of voters and results of the votes with the voters who cast. This voting system is unsuitable for use in a general election. All e-Voting system paperless could suffer the same flaws, despite any “certification" it would have been other-wise. In [35], it was suggested that the best solutions are systems with an “audit trail voter verifiable," where an e-Voting system might print a ballot that can be read and verified by the voter votes.

Spoofing; Sites spoof malicious Web sites that are created to look like legitimate Web site, in a scenario of voting it is understood that this could be really bad, the site could be used to launch phishing attacks to collect credentials voters as a PIN or password required to vote. The website may look exactly like a voting site in the state, but redirect the browser to the voter to a malicious Web server. There are many ways that an attacker could spoof a legitimate site vote. One way might be to send emails to users tell users to click on a link, which then set up a voting site were false adversary could collect the credentials of the

user, to steal the vote, and then use it to vote differently. An attacker could also establish a connection to the legitimate server, feed the user a fake web page, acting as a man in the middle, transfer, and control all tracks between the user and the web server. Transferring information between the user and the server, the user's voice can be changed before further sent to the server. [7, 10].

Malicious Payload; Threats of a modern system of e-Voting security: Malicious payload is a threat to the security of the personal computer of the voter. The malicious payload is software or configuration to damage and could be a virus, worm, Trojan horse or a remote control program that is perhaps the greatest threat in a scenario of voting. If a malicious program is installed on the computer of the voter, it could change the secret ballot. The owner of the computer may not be aware of even have one installed because these programs can be di cult to detect (run in stealth mode) malware. Malware of this kind have increased in sophistication and automation in recent years in a way that they can do more damage, more likely to succeed and to dress better. Even if a system of Internet voting has strict protocols for encryption and authentication, malicious code can do its damage before the other security features are applied to the data. [10].

4. Attacks

E-Voting technology can speed the counting of ballots and provide better accessibility for disabled voters. However, e-Voting could also facilitate electoral fraud [10]. Internet based voting systems require strong safeguards against hacking attacks, viruses and Trojans. Software continues to get complex and can never be bug free. A virus or network attack can also be mounted during the verification process and result in false positive verifications. Network attacks may be met by cryptographic key exchange and distributed back-end databases. Information dispersal algorithms and verifiable secret sharing schemes may be used to maintain system fairness such that no single server stores all the cast ballots and the partitions are distributed over independent servers. As long as a majority of these servers remains honest, the possibility of sabotage remains low.
Initiated in a voting system may include hardware vendor and/or pre made software, election officials, poll-workers, maintenance technicians, and others. It is impossible to completely prevent internal attacks, but levels of resistance to such attacks systems [36].
Attack on e-Voting system can be classified according to the configuration; attacks such as advertising, pro t attacks, terrorist attacks and attacks that are motivated by the desire to create instability in the state government and more. Because of the safety pro le at high risk of e-Voting, it is necessary that each component or unit in the electoral process presents the principles of security (confidentiality, integrity, availability) and controls must be applied to protect them. E-Voting requires the implementation of protective measures to fight against all identified threats and the ability to prevent unregistered. An attacker must have three things:
Reason The reason for wanting to attack.
Possibility time and access to a full attack.
Method the knowledge and tools necessary to perform an attack skills.

Attack on an e-Voting system can be classified according to the model; these attacks are attack ads, non-profit force attacks and terrorist attacks are motivated by the creation of the instability of the current government/democracy. Threats could be, for example internal vendor, election officials. Alternatively, they can be external, such as individuals, organizations and funded, states, parties, criminals, terrorists, many of whom cannot even be prosecuted. The motivations of attackers ranging from advertising, foreign intelligence and terrorist acts, governments handling system to their advantage [9].

Voting systems based on the Internet are vulnerable to attack by three main points; the server, the client and the communication infrastructure. Penetration attacks target the client or server directly while DoS attacks target service and interrupt the communication link between the two. The penetration attacks involve the use of a distribution mechanism for carrying a malicious payload to the target host in the form of a Trojan horse program or a remote control. Once executed, it can spy on the ballots, prevent voters from casting ballots, or worse, change the ballot according to his instructions. Remote control software can compromise the secrecy and integrity of the ballot by those who monitor the activity of the host.
In the context of new voting technologies (NVT), piracy is seen as an entry in the illegitimate system made by anyone external to the process management. For DRE voting systems and scan ballots, safeguards must be put in place to prevent physical handling with appliances. Election Observation Mission (EOM) must check, for example, the USB ports or other external connections are not easily accessible. In addition, the storage and transport of NVT devices must be conducted in the context of secure protocols defined manner, and access to peripherals must be observed when they are not in use, with appropriate records kept. Hacking can also occur if the devices are connected to the Internet [37].
Another challenge is the need to preserve the secrecy of the vote, while at the same time the integrity of the results. It has hitherto been di cult for e-Voting process - especially Internet voting - to meet these two fundamental principles of democracy at the same time. Another

challenge is that NVT present additional difficulties in the electoral process, such as the need to amend the legislation; planning how NVT will be acquired, tested, evaluated, certified and secure; and provide education and training of electoral agents voter; and general as to the transparency of the process and access concerns for observers. Using NVT therefore not necessarily built trust; rather, it seems to require existing confidence in the administration of elections for successful implementation. These challenges, if they are not fully taken into account, can weaken public confidence in the electoral process.

In addition to physical intrusion, external hacking is a particular threat. The EOM should check how the system prevents or detects an illegitimate access, and should assess the likely effectiveness of these measures. In Internet voting systems, the EOM should consider how the system verifies the identity of the voter and the threats that could create potential. In addition, the overall protection of information from unauthorized access, through the use of trans-mission lines dedicated firewall and overall concepts of external security access systems, should be considered. Data manipulation by officials, suppliers or electoral technicians is another potential threat posed by NVT. The EOM should ensure that procedures are in place to limit the ability of any person to undermine the system. For example, there should be a division of labor within the electoral administration to minimize the possibility of an internal manipulation. The physical and electronic access to the NVT system must be strictly regulated by written procedures. Any access should be limited and observable so that election officials or suppliers have access only to components that fall within the scope of their responsibilities. The EOM should also check if sensitive system operations are performed by more than one person and a record of all transactions is maintained. Safety procedures must be both effective and fully implemented; the measures that bring evidence justified as inviolable security seals with unique numbering, secure stamp documents and similar mechanisms to prove the authenticity of procedures to provide security against malpractices. Although these security measures are necessary, they may not be sufficient to ensure electoral integrity or to maintain public confidence. Appropriate verification measures, including audits of voter -verified paper documents are needed to fully guarantee the integrity of the vote [38].
In practice, the two most important problems of computer security compromise and coercion. Cryptography cannot protect a voter coercion when voting from home or a public place, but the system must include features to prevent coercion. A solution to the problem of stress is the ability to submit multiple ballots. The system allows the voter to multiple re-vote the final ballot. It is also possible to vote at the polling station and a ballot crush any e-Voting, no matter what the time stamp (submitted before or after e-Voting shown). The previous question is a measure against coercion external attackers, but stress can also be done by election insiders/employees. A voter authenticates before launching a ballot, and election officials with access to the authentication sys-tem can detect any electronic e-Voting by a voter. The election officer cannot see the contents of the ballot cast, but he could see/detect constraint voter casting a new vote. An election official coercing access to ballots counted could also verify that the voter constraint (s) (the victim (s)) does not have to vote again.
If forcing the voter (s) to submit a ballot with the desired effect coercion can observe the counted ballots and verify if the ballot (s) are present among them. The compromised computers come home is another major threat. A significant fraction of home computers is compromised, and the Norwegian protocol must provide the voter an opportunity detect falsification ballot without relying on computers. It is complicated, because the voter cannot perform cryptographic calculations without a computer, and this was the method of using a generator and receiver codes pre-generated receipt is involved. The voter receives reception codes pre-calculated on his voting card with his voting card and after casting a ballot, receiving codes generated by the generator and receiving the ballot box is sent to the voter by not the system and the computer, but through an independent channel (postal service). If the computer voter is corrupt, the attacker may be able to see the ballot, and the attacker can also change the ballot. There-fore, these security mechanisms allows the voter to note manipulation with high probability [10].

4.1 Physical Attacks

Many physical attacks can be made on the e-Voting system to sabotage the election. Vandalism of e-Voting systems makes it unusable for Election Day. Saboteur can remove network connections and pull the plug on e-Voting systems causing lost votes. Attackers can remove hard disks or smart cards to replace falsified data. E-Voting machines could be stolen by attackers discover information confidential voting on users [23].

4.2 Overloading Attacks

Denial-of-Service (DoS) Attack Distributed Denial-of-Service (DDoS) attack is an attack on a computer system or a network in which a simple auto-mated request is repeated at a very high frequency, with the aim of overloading the connecting lines of the system or the calculation of capabilities. These attacks are detectable and may require the postponement of the election. EOM should therefore check what security measures were put in place to protect systems against such attacks [39].

DOS attacks are performed by automatically sending a flood of messages on a website, server, or on a channel similar to crash or reduce the quality because it cannot handle all the traffic generated. Using a DOS attack distributed (DDOS), attackers can cause routers to crash or electoral servers being flooded, or it is possible to attack a large number of hosts such demographically targeted to stop the operation of the election. This can be a major threat to Internet voting if such voting takes place in one day. It is important to have additional bandwidth to handle the traffic and some voting systems I will describe later, the vote may occur over several days in advance of the election [10, 40, 41, and 42].

Ping of Death The ping of death relies on a flaw in some Transmission Control Protocol, Internet Protocol (TCP/IP) stack implementations. The attack relates to the handling of unusually and illegally large ping packets. Remote systems receiving such packets can crash as the memory allocated for storing packets over flows. The attack does not affect all Systems in the same way, some systems will crash, and others will remain unaffected [23].

Packet Flooding Packet flooding exploits the fact that establishing a connection with the TCP protocol involves a three phase's handshake between the systems. In a packet flooding attack, an attacking host sends many packets and does not respond with an acknowledgement to the receiving host. As the receiving host is waiting for more and more acknowledgements, the buffer queue will fill up. Ultimately, the receiving machine can no longer accept legitimate connections [23].

4.3 Receipt Attacks

Trash Attack The idea of the trash attack is that if voters throw away their (paper) receipt, then authorities who find these receipts could conclude that these voters will not check their receipts on the bulletin board, and hence, ballots of such voters can safely be modified [27].

Clash Attack; the simple idea behind the shock attack, is as follows. Voting machines are trying to provide different voters with the same reception, where the name of the attack. Accordingly, the authorities can safely replace the ballots news on the scoreboard; therefore, manipulate the election without being detected. In [27], it was shown that, surprisingly, many e-Voting systems that have been designed to provide the verifiability between systems that have been used in real elections are vulnerable to this attack, under realistic assumptions of trust in machines and authorities vote. Our results show that this attack is a potentially dangerous attack for a large class of e-Voting systems. It must be noted that the shock attack can work even if the voters and election observers know exactly how and what the electorate voted. So confront attacks are different and more subtle than the known ballot stuffing attacks (see, for example, attacks ballot stuffing) [27].
This attack does not seem to have attracted much attention in the literature. Even if the attack is quite simple, under reasonable assumptions confidence, it applies to several e-Voting systems that have been designed to provide verifiability. In particular, it applies to large as well as two e-Voting systems that have been deployed in real elections and voting systems Three Ballot and Vote/Anti-Vote/Vote (VAV), the Wombat voting system and, its alternative voting system Helios [27].

4.4 Man-in-the-Middle Attack

Fraud in the form of fake servers must also be taken into account. Some server may pretend to be the official server by tampering with the DNS or by using a name very similar to that of the official server (Man-in-the-Middle). To protect the system against Man-in-the-Middle attacks, a digital signature may be applied to the ballot to ensure verification of the voter submitting the ballot. However, it is of utmost importance that the confidentiality of the vote is not threatened [4.43].

5. Conclusion and Future Work

From the previous section, it seems that online voting is very promising for application in Egypt despite of the existing challenges. Implementing an online voting system offers many advantages. One of the most important advantages is its ability to increase voter turnout by making the elections more convenient and more accessible to busy voters, lazy voters, and voters with special needs. Other advantages include the low cost, ease of administration, and auditability. The difficulty of applying online voting in Egypt lies in convincing voters that their privacy is maintained at all times. Public must be informed about the manner by which the Internet is protected from outside influences, including national and international hackers as well as whom might try to cast more than one ballot. In addition, online voting may require some legal regulations to be applied in Egypt.
We are working on developing a complete end-to-end auditable online voting system that is capable of satisfying all the requirements of e-Voting, getting over the technical challenges, surviving against possible attacks, complying with legal regulations, and gaining the confidence of the Egyptian people.

Acknowledgement

I would like to express my appreciation for the support I got from Egyptian Ministry of Foreign Affairs and all the help I received from George Town University Library;

they gave me the chance to access the latest publications in the field.

References

[1] J. Pujol-Ahull, R. Jard-Ced, and J. Castell-Roca, "Verification systems for electronic voting: A survey," pp. 163–177, 2010.
[2] S. Caarls, E-voting Handbook: Key Steps in the Implementation of E-enabled Elections. Council of Europe, 2010.
[3] A.-M. Oostveen, "Outsourcing democracy: Losing control of e-voting in the Netherlands," 2010.
[4] "Electronic voting - challenges and opportunities," 2004.
[5] M. Iwasaki, "E-voting in japan: A developing case?" in 4th International Conference of Electronic Voting, vol. 167, 2010, pp. 283–295.
[6] H.-W. Lee, "Political implications of e-voting in korea," vol. IX, no. 1, pp. 91–107, 2005.
[7] M. F.M.Mursi, G. M. R. Assassa, A. Abdelhafez, and K. M. Abo Samra, "On the development of electronic voting: A survey," vol. 61, no. 16, pp. 1–11, 2013.
[8] L. Fouard, M. Duclos, and P. Lafourcade, Survey on Electronic Voting Schemes, 2007.
[9] D.Zissis, "Methodologies and technologies for designing secure electronic voting information systems," 2011.
[10]M. Stenbro, "A survey of modern electronic voting technologies," 2010.
[11]L.Mitrou, D. Gritzalis, S. Katsikas, and G. Quirchmayr, Chapter 4 E-VOTING: CONSTITUTIONAL AND LEGAL REQUIREMENTS AND THEIR TECHNICAL IMPLICATIONS, 2009.
[12] Eric A. Fischer and Kevin J. Coleman, "The direct recording electronic voting machine (DRE) controversy: FAQs and misperceptions," 2005.
[13] M. Abo-Rizka and H. Ghounaim, "A novel in e-voting in egypt," vol. 7, no. 11, pp. 226–234, 2007.
[14]Abdalla Al-Ameen and Samani A. Talab, "E-voting systems security issues," vol. 3, no. 1, pp. 25–34, 2013.
[15]T.R¶ssler,"E-voting: A survey and introduction," 2009.
[16] R. Kofler, R. Krimmer, and A. Prosser, "Electronic voting: algorithmic and implementation issues," in Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003, 2003, pp. 7 pp.–.
[17] M. Bishop, "An overview of electronic voting and security," 2003.
[18] S. Delaune, S. Kremer, and M. Ryan, "Verifying properties of electronic voting protocols," in Proceedings of the IAVoSS Workshop On Trustworthy Elections, 2006, pp. 45–52Proceedings of the IAVoSS Workshop on Trustworthy Elections. 45-52, 2006
[19] Jan Gerlach and Urs Gasser, "Three case studies from Switzerland: E-voting," 2009.
[20] Bryan Schwartz. (2013) Establishing a legal framework for e-voting in Canada.
[21] I. Ray, I. Ray, and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the internet," in Advanced Issues of E-Commerce and Web-Based Information Systems, WECWIS 2001, Third International Workshop on., 2001, pp. 188–190.
[22] P. Heindl, "E-voting in Austria legal requirements and first steps." pp. 165–170, 2004.
[23] A. Al-ameen and S. Talab, The Technical Feasibility and Security of E-Voting, 2011.
[24] Lilian Mitrou, "ELECTRONIC VOTING OBSERVATORY II VOTOBIT," 2004.
[25] Christine Lai, "The impact of voter identification laws on voter participation," 2013.
[26] Rodney Smith, "Multiple voting and voter identification," 2006.
[27] R. Kusters, T. Truderung, and A. Vogt, "Clash attacks on the verifiability of e-voting systems," in 2012 IEEE Symposium on Security and Privacy (SP), 2012, pp. 395–409.
[28] O. etinkaya and D. etinkaya, Anonymity in E-Voting Protocols, 2008.
[29] Robert Krimmer and Melanie Volkamer, "Observing threats to voter's anonymity: Election observation of electronic voting," 2006.
[30] D. Chaum, P. Y. A. Ryan, and S. Schneider, "A practical voter-verifiable election scheme," in Computer Security ESORICS 2005, ser. Lecture Notes in Computer Science, S. d. C. d. Vimercati, P. Syverson, and D. Gollmann, Eds. Springer Berlin Heidelberg, 2005, no. 3679, pp. 118–139.
[31] L. Langer, A. Schmidt, M. Volkamer, J. Buchmann, and T. U. Darmstadt, in Classifying Privacy and Verifiability Requirements for Electronic Voting, 2009, pp. 1837–1846.
[32] P. Delwit, E. Kulahci, and J.-B. Pilet, "Electronic voting in belgium: A legitimised choice?" vol. 25, no. 3, pp. 153–164, 2005.
[33] D. D. Cock and B. Preneel, "Electronic voting in Belgium: Past and future," in E-Voting and Identity, ser. Lecture Notes in Computer Science, A. Alkassar and M. Volkamer, Eds. Springer Berlin Heidelberg, 2007, no. 4896, pp. 76–87.

[34] Michael Ian Shamos, “Electronic voting glossary,” 2011.
[35] T. Kohno, A. Stubblefield, A. Rubin, and D. Wallach, “Analysis of an electronic voting system,” in 2004 IEEE Symposium on Security and Privacy, 2004. Proceedings, 2004, pp. 27–40.
[36] J. Epstein, “Internet voting, security, and privacy,” vol. 19, no. 4, p. 885, 2011.
[37] R. Krimmer, “Handbook for the observation of new voting technologies,” 2013.
[38] M. Volkamer, Evaluation of Electronic Voting - Requirements and Evaluation Procedures to Support Responsible, 2009.
[39] Sandeep Mudana, “Security flaws in internet voting system,” 2004.
[40] Darshan Lal Meena, “Effects of DoS attacks on the e- voting system and feasible measures to prevent them,” vol. 3, no. 4, pp. 16–21, 2014.
[41] Volkamer, M.: Evaluation of Electronic Voting - Requirements and Evaluation Procedures to Support Responsible, 2009
[42] Electronic Pool Book systems as distributed Systems: requirements and Challenges (national Conference on state certification testing of Voting systems may 19-20, 2015, WA, US.
[43] Issues and challenges of transition to e-voting technology in Nigeria, International Knowledge Sharing Platform, Public policy and administration research 2015