ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 7, Issue 2,February 2020

Survey on Efficient Electoral Polling

Sherif T. Amin

Assistant Professor, Department of Computer Science, College of Computer Science and Information Systems, Jizan University, Jizan, KSA.

ABSTRACT: The first round of the Tunisian presidential election will take place on September 15, 2019, according to what has been published by the Independent Higher Electoral Commission (ISIE), the second round will be organized before the date of 03 November 2019. Adopting new technologies to install a true electoral democracy in Tunis might be a challenge. This paper studies 3 forms of distant polling in an unrestrained location: Internet polling, hybrid postal polling and postal polling. It breaks down polling processes into different stages, comparing weaknesses in respect of a democratic vote criteria (confidentiality, anonymity, transparency, uniqueness, sincerity). Whether it's reliability or safety, each vulnerability is measured by 3 parameters: scale, difficulty and visibility. The study finds that the automation of treatments combined with the dematerialization of polling objects tends to replace visible weaknesses of reduced magnitude with obscured and large-scale weaknesses.

KEY WORDS: Virus, Worm, Internet Polling, Democracy.

I.INTRODUCTION

How elections were conducted in the 19th century? How did elections work in the modern age and how should we vote in the 21st century? (Fig 1) shows a painting from 1846 that depicts an election from the mid-west in the USA. There is a voter in the red shirt telling his vote to the election judge behind on the porch, you can also see the tabulators making marks on a piece of paper. This works okay but it has some problems and there is a person whom already voted, and he's been paid off with a glass of whiskey and voting is out loud in the presence of everyone, moreover if tabulators disagree at the end of the day on their vote counts there's no balance to recount so there are problems in the reliability of the election.

Fig 1. Elections in the 18th century

So, kind of flaws in out loud voting like this are the lack of the secret ballot which permits voters to be bribed or coerced and the inaccuracy due to the inability to recount. Paper ballots started to be used in the US in the 19th century (Fig 2 (a)) shows an early paper ballot where you can see that the voter has just written in the names of the candidates, the ballot itself was printed as an advertisement in the local newspaper probably by Francis Gehon where you can see he put his own name in as a candidate for the first office for delegate to Congress. By the late 19th century paper ballots look like (Fig 2 (b)) where the party would print a straight ticket ballot listing all the candidates of that party and a voter would bring in the party ballot of his choice and deposit it in the ballot box.

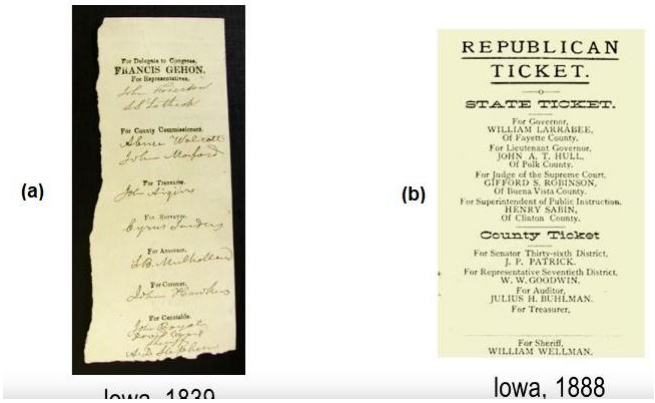
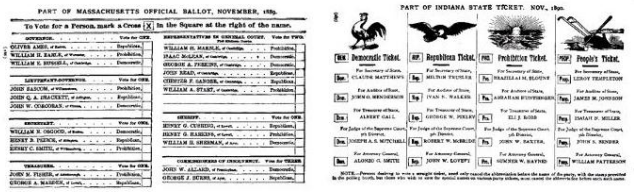


Fig 2. Early paper ballots

So, it looks easier to be recounted but it still some problems, first of all, voters can bring their own ballots, so why not bring 10 and stuff them all in the ballot box instead of one if you can get away with it. Also, the party could print their own ballots in different colours so they tell who is voting for whom, so there are a lot of problems with election fraud and corrupt political machines in the 19th century. This led to technological and political reforms in the voting process to guarantee vote count even if no individual is trusted to count up the votes, and also the secret ballot to prevent coercion and bribery of voters. This is a kind of computational protocol that computer scientists can analyse it. Doing these two things together providing an accurate vote count while making it impossible to learn how any individual voters voted is not trivial technology, voting protocols had to be invented, so what we need is:

- each person can vote exactly once
- accurately record the votes
- accurately count the votes
- that the voter can be sure that his vote is counted even without trusting the other side people but sometimes the other side people are the elected officials that are running the election elections
- and secrecy that you can't learn how a person voted against his/her will but even more you can't learn how a person voted even with his/her cooperation because if you can ask him/her to cooperate then you can coerce or bribe the voter so there must be no way for the voter to prove how he or she voted.

Here's the technology it's called the Australian paper ballot (Fig 3) it's a pre-printed ballot with the names of all the candidates and you just mark an X next to the name of the candidate you want. It seems perfectly obvious because it's the way we're used to vote for the last hundred and twenty years but it had to be invented just marking X and because we are marking an X which is pretty much indistinguishable from somebody else X so it's difficult to associate the particular ballot from a particular person.



From *ELEMENTS OF CIVIL GOVERNMENT*
by ALEX. L. PETERMAN, Kentucky State College, 1891

Fig 3. Australian ballots

The rest of the technology include the voting place (Fig 4) to vote or enters over there and signs in implies voter registration which didn't really exist much earlier than 1890. You can notice that there's two people at the sign-in table a representative of two different parties, they want to make sure that together they allow only a legitimate voters and only eligible voters. Voters handed a ballot at that point control over the number of ballot papers helps avoid ballot-box stuffing the voter goes to the privacy booth to mark the ballot if we thought shoulder surfing was only invented in our lifetime that's not true there is important safeguards including the railing shown in the same (Fig 4) to preserve the secrecy of the ballot. Voter approaches the ballot box to put the ballot in it, but again there is more of one person there, the representative of different political parties who don't trust each other but who can watch that ballot box, they can see it is empty at the beginning of the day, they can see that each voter puts just one ballot in, they can see that nobody else has put ballots in, some of those with a bell that rings every time you open up the slot to put a ballot in.

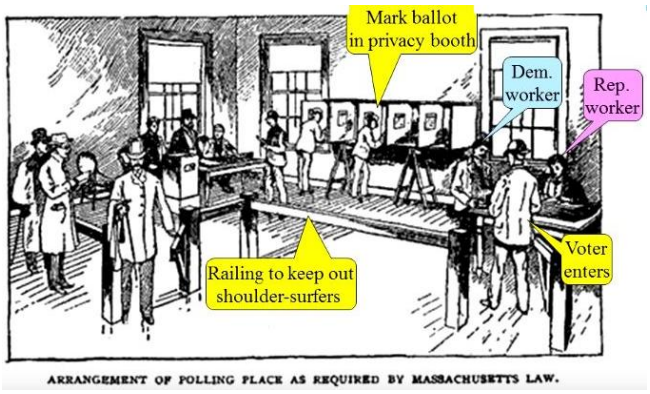


Fig 4. Polling place

This is technology, it had to be invented so what you get out of all of this technology is a protocol where and we can trust the result of the election even though we don't trust any individual who is running the election. One problem though is that counting up those balance by hand even in the presence of witnesses can still be inaccurate and especially when there are a lot of different offices being in the same election. Each ballot is marked by many different people which makes it difficult to count, so people wanted to mechanize the process. The first mechanized machines were invented around 1890 as well they're very high-tech for their age here's a 1936 machine. (Fig 5)

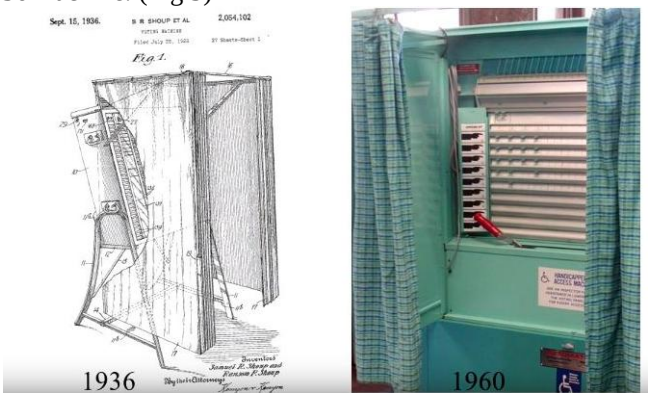


Fig 5. Mechanical voting machines

Unfortunately, even with these high-tech machines; we know how to make them cheat. There's a pencil shaving trick there is a grease trick there's a wire trick there's a paper trick, but a lot of the ways you make it cheat end up with an undervote. Some of the votes don't get counted as you make them cheat. One way of making it cheat is by transferring votes from one candidate to another, that seems such not a great thing, the failure to count lots of people's vote, but at least when it happens there is evidence that something fishy is going on and then we can revisit your election protocol before the next election. If these machines get rigged, they work the same way when it's after 7 a.m. as it is before 7 a.m. so you can test them before the election starts and then pretty much work the same way after the election goes on, except for the pencil shaving trick okay. So, by the 1970's people started to vote on optical scan paper ballot (Fig 6) where we fill in the bubble next to the name of our candidate for each office and we feed the optical scan paper ballot into the machine over there and it counts the votes electronically.

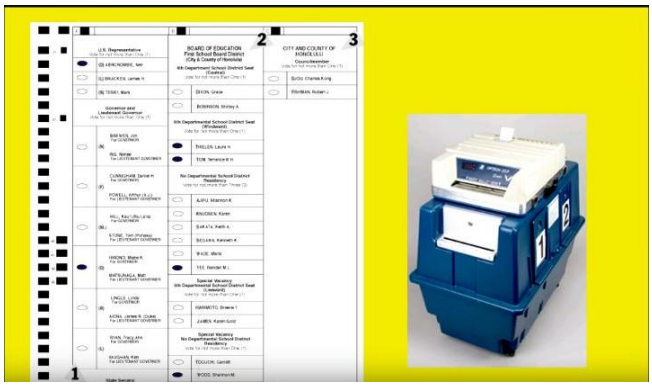


Fig 6. Precinct-count optical count

Towards the 1990s computerized touchscreen machine voting machines were invented. (Fig 7) shows a whole bunch of touch-screen voting machines. There's a problem with these touch screen computers voting machines whoever writes the computer program that's installed in it gets to decide who wins the election.

Fig 7. Touch-screen voting machine

In the 21st century distant polling practices have been improved by automatically scanning ballots or dematerializing the objects of polling in an Internet polling location. This paper situates three techniques of distant polling (postal, hybrid postal, and Internet) polling, demystifying the details and establishes the different phases. Internet polling technical flaws are exposed in the second and third part whereas the fourth part makes a comparison of the weaknesses of each of the polling techniques.

II. DISTANT POLLING

A. Definition

Depending on region or country, distant polling can refer to two distinct concepts:

- Polling outside its usual polling place but in a place under surveillance (such as the premises of an embassy);
- Votes in an unrestrained location and in the absence of an electoral supervisor.

Distant polling beyond the control of an electoral supervisor is our concern in three forms: (Internet, postal and hybrid) polling. The scope of an election study can go as far as to include the preparation of electoral lists, the campaign of candidates or the proclamation of the results. We focus only on the ballots from the communication of polling materials to electors to the counting of polls. We will not present here the issues related to the ritual of polling that have already been widely addressed (see for example [5] and [14]), nor the aspects concerning the digital divide or accessibility (see [1], [13]).

B. Three forms of distant polling in an unrestrained location

For each of the distant polling forms we focused on defining a model embodied by a genuine application used on a large scale and which can be considered practices already implemented or awaiting to be implemented in the field: (Internet, postal correspondence, and hybrid postal) polling.

- *Internet polling:* Internet polling (Fig 8) is part of a larger group called electronic polling (e-poll). E-poll groups all practices of polling encompassing an electronic apparatus (polling computers, poll by kiosk, etc.). There are draft sets of international standards, but these lack accuracy in defining the necessary legal, organizational, and technological standards, so Internet polling has many variations.

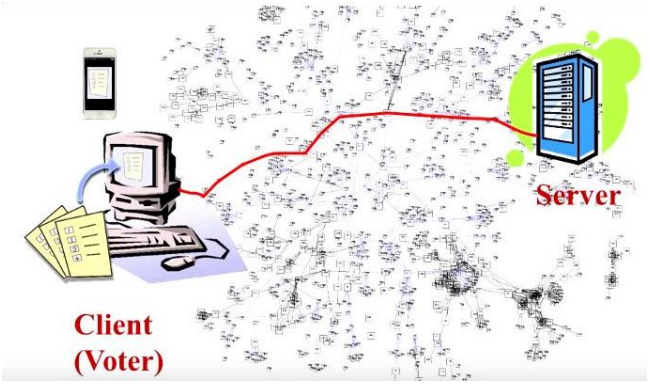


Fig 8. Voting on the Internet

However, here is the general scheme that is followed by the usual so-called secure Internet polling processes, information useful for authentication is communicated to electors by mail. Electors log on to an official polling site from any Internet connected computer with a polling app compatible browser operating on the authorized website. They must then provide their identity and then authenticate themselves (prove their identity) before expressing their choice, which will be encrypted and then forwarded to the server housing the official polling website that accumulates the polls, stocks them until the election's end. Results will be produced at the close of the election. Since not all electors have an Internet-connected computer, postal mailing polling process needs to be always available.

- *Postal Correspondence Vote:* Each elector receives polling materials in the mail. It includes a "vote card" bearing the elector's identity, the ballot, an unmarked envelope and a mailing envelope. To elect, the elector puts his chosen ballot in

the unmarked envelope, then seals that envelope, as well as the polling card after signing and dating it, into the mailing envelope. This envelope is then mailed to the central elections' office. The polling centre collects received envelopes. Counting occurs in two stages. The signature register removes the electors' names and the mailing envelopes are unsealed to amass the unmarked envelopes which are then randomized so as to remove any connection between them and the mailing envelopes. Finally, polls are counted to establish the final election's result.

- *Hybrid Postal Polling: Postal and Computer Counting:* The hybrid postal polling process is an adjustment of the postal mailing polling process to automate counting through computers' exploitation. Electors receive polling materials by mail: a "polling card" and one envelope. Each polling card has a mark (barcode or number) to recognize the elector and a list of boxes symbols one for each proposed candidate that the elector blackens to signify his choice (Fig 9). On the election day ballots are taken out from their envelopes, counted, and then scanned by an optical reader (Fig 6) that updates the signature register and the polls acquired for each candidate.

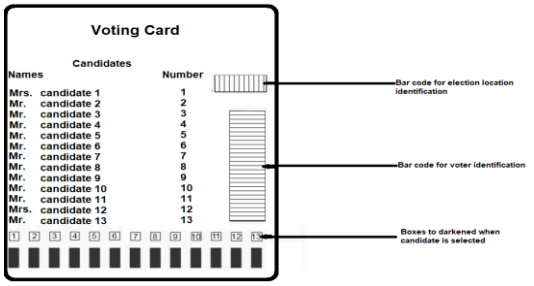


Fig 9. hybrid postal mailing polling card

C. Stages of Distant Polling in an Unrestrained Location

Postal polling in an unrestrained location can be divided into several abstract phases, common to all 3 polling techniques, but differently implemented according their modalities (table 1): the polling organizers organize the polling material (O1), and its transfer to electors (O2). Polling material moves through the transfer channel (T1) and reaches the elector (V1). The elector expresses his choice (V2) and then prepares to send his vote (V3). The vote is transmitted (T2). Polls are received by the polling station (O3) which then executes the counting process (O4) (Fig 10). This presentation does not reflect all communications; for example, during an Internet vote there are exchanges between the elector and the polling system when expressing their choice.

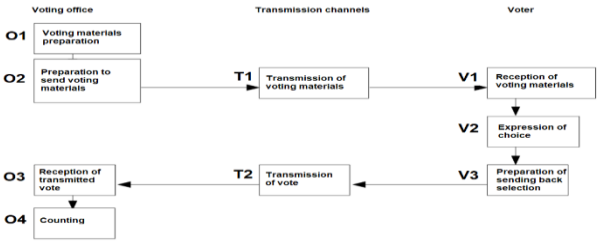


Fig 10: The phases of distant polling in an unrestrained location

Table 1: Phases of distant polling for 3 polling forms in an unrestrained location

		Internet Polling	Postal mailing polling	Hybrid mailing polling
O1*	**Polling materials preparation**	Developing signatures of users' IDs and passwords, printing polling materials	Printing polling materials	Printing polling materials
O2*	**Preparation to send polling materials**	Folding and mailing		
T1*	**Transmission of polling materials**	Connection IDs are routed (postal mail)	Both envelopes and ballots are routed (postal mail	Both envelope and poll card are sent by (postal mail)
V1	**Reception of polling materials**	Elector receives the polling materials.		
V2	**Choice Expression**	Elector logs on to the election site, identifies himself, authenticates himself, makes his choice and validates it.	Voter expresses choice using the poll card	Voter expresses choice using the ballot paper
V3	**Preparation of sending back selection**	Virtual polling card gets encrypted	The elector puts his ballot in the unidentified envelope, and the ballot in the mailing	Voter puts his ballot in the mailing envelope
T2	**Transmission of vote**	Network carries polling card to the polling collection facility	The envelope is sent to the polling station	
O3	**Reception of transmitted vote**	Polling collection facility saves polls` envelopes received, updates the list of signatures and sends receipts back to electors	The polling station receives and stores the polling envelopes	
O4	**Counting**	Software decrypts polls then counts them	Signatures list is updated, polling envelopes gets opened and then polls are counted	Envelopes gets opened, the optical reader reads the ballots, the software updates the signatures` list, and then counts the polls.

**This step might not exist when electors log in using a magnetic track connection card.*

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

III. METHODOLOGICAL CHOICES

A. Comparatives approach

All polling systems have weaknesses, no ideal polling system guarantees rigorous adherence to the principles of democratic election and gives perfectly accurate results. Our study will evaluate several standards of distant polling according to benchmarks expressed by different international organizations: Universal Declaration of Human Rights of 1948], Code of Conduct in matters, the Organization for Security and Cooperation in Europe's (OSCE) election observation manual. These benchmarks may be specific to any democratic poll or may be restricted to postal polling. The aim is to measure the significances of major poll vulnerabilities in the following three parameters: significance, difficulty and visibility.

- *Significance* depends on the number of polls possibly affected by fraud or malfunction. This factor can acquire few, or average number of polls enough to change the result of the elections, or possibly almost all polls.
- *Difficulty* is a fuzzy estimate of the likelihood of occurrences of the conditions necessary to exploit the vulnerability. In the case of a technical reliability problem, it is a matter of estimating whether the failure is common or rare. For a fraud it is necessary to measure the complexity of its successful implementation (number of people involved, technical knowledge, discretion, etc.). This setting can take the 3 small, medium and large values.
- *Visibility* determines whether the consequences of weaknesses are noticeable. It can take all 3 values: zero (obscured consequences), average (visible but unproven consequences) or large (visible consequences that could cause the election to be cancelled).

Worst situation occurs when large magnitude comes alongside zero visibility and small difficulty. These three conditions are dependent: visibility and difficulty will only be expected for medium-sized or large incident.

B. Distant Democratic Vote

1. Democratic vote: Distant polling is a segment of democracies-based authority processes. The measures specified by international bodies aim to respect democratic elections principal values:

- *uniqueness*: one vote per elector;
- *confidentiality*: each elector can make their choice in secret;
- *anonymity*: hopelessness of tracing back a ballot to the elector who chose it;
- *sincerity*: election's results faithfully reflect the electors' desire;
- *transparency*: "For Internet polling, the transparency of the system must be guaranteed, in the sense that its proper functioning must be able to be verified".

2. Distant Polling: These standard measures are accompanied by conditions specific to distant polling:

- *safety*: system can tolerate deliberate attacks;
- *reliability*: system works, regardless of software or hardware inadequacies.

Ensuring the accuracy of the polls results and its availability between the time of the electors' will expression and the polls counting, remains one the major challenges.

VI. TECHNICAL FLAWS IN INTERNET POOLING

Internet polling is a new process depicted by the dematerialization of all polling objects (ballot box, polling ballots, and signature book). We detail few technical weaknesses that could alter the virtual features representing the polling. These weaknesses may be a matter of safety or reliability. The client machine is a computer or a phone it's connected over the internet to a server machine. We might worry about whether our votes are being corrupted in transit by some hacker, so the usual way is by ensuring against that by using end-to-end encryption between the client and the server so that the hacker can't see what's in the packet and can't change what's in the package because of cryptographic authentication. But what we would worry about is who installed the vote counting program in the server machine just like with the touch-screen voting machines. Whoever installed the program that counts the votes decide what algorithm is used to report who wins, that programmer thought that he got to install the program in the server but his program has to run in an operating system that's really the operating system that decides what program is running the operating system is installed by a bootloader and there's so many layers of software all the way down that it's hard to really have control of what they are and to believe that state or county election official can be served on top of the entire software

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

stack that's just beyond belief. In fact, even if the voting program and the operating system were honest and all the software in the server we're completely legitimate that would only be true until somebody hacks into the server and replaces the counting software. That's a real problem can servers on the internet really be hacked of course. The District of Columbia in 2010 decided to conduct their local elections online with an internet server and they invited the public in a pilot two weeks before the real election in a mock election to see if they can hack it. So, a team from the University of Michigan took up the challenge and with very little difficulty they really break in and hack the system. (Fig 11) shows the district of Columbia's server setup.

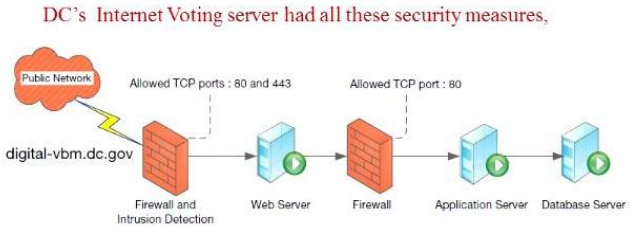


Fig: 11Voting test hacked by hackers

As you would do if you were writing a secure server we put a firewall out here with intrusion detection algorithm, there's a web server in between the web server and the actual data you put another firewall where our vote counting server is located, there is the database this is all conventional well-organized computer security but still the hacking team were able to hack in. They just exploited software vulnerabilities in the firewalls and in the web server they were able to own that system, they stole all the voter registration information, the voters' personal information, they changed votes, they packed the software so that when your vote was finally recorded it would play the University of Michigan fight song, they controlled the cameras in the server room watching the people running around frantically trying to figure out what was going wrong, only after they announced that they hacked it. Because after they hacked it and before they announce publicly that they hacked it, they could see from the cameras in the service room that nobody was worried about anything, nobody can tell when his server is being hacked. We should also worry about vulnerability in the client, (Fig 12) the client user interface is an interface where you record what your votes are supposed to be, that user interface might just be telling you yes boss and then send whatever votes over the Internet, how do you know that's not happening, so whoever installs the client's vote user interface gets the control really what votes are sent regardless of what it says it is recording. Whoever installs the phones operating system decides which version of the vote counting software is installed and there's layers upon layers there and even if those people are completely honest the hacker on the internet might be hacking on your phone or computer and changing what that software does.

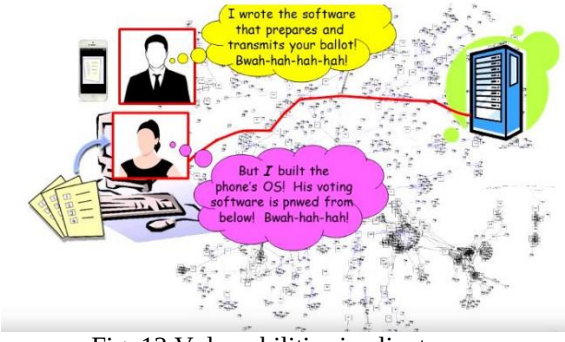


Fig: 12 Vulnerabilities in client

Here are all the questions you can ask about Internet voting and most of them don't have answers:

1) Are ballots transmitted correctly? (Maybe)
2) Can eavesdroppers learn how you voted? (Probably not)
3) Does the server software add up the votes correctly? (Well if it has not been hacked or if it's not fraudulent to begin with)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

4) Are the votes displayed on the screen the same as the votes actually transmitted by the client software? (Depends on what the client software does.)
5) Is the real server software actually installed on the server computer? (Who knows?)
6) Am I talking to the real server or is it an imposter?
7) How are the voting credentials distributed (the pin number) to voters?
8) Is the person here who typed the pin the actual voter?

it's only unsolved problems here, so we need to remember what a voting protocol needs, all the criteria previously mentioned to accurately conduct the elections even without having to trust any particular person and guaranteeing a secret ballot these are not really solved for internet voting computer.

Computer scientist cryptographers are currently working on cryptographic voting protocols that probabilistically guarantee the accurate counting votes and the ability to tell that your vote counted without being able to prove how you voted but these protocols are not really ready for prime time and almost all of the Internet voting vendors are not selling you fancy cryptographic protocol that try to achieve all these things they're just some new software that adds up to vote unless it's been replaced. So, when we see internet voting discussed it's the internet voting we have today not the end of voting that we might have in the future if this scientific research pans out and that's a big worry.

C. Security

1) Worms and Viruses: The position from which the elector polls is likely to harbour worms and viruses capable of triggering targeted attacks aimed at the expression of the elector's vote. Since most antiviruses can identify only known viruses and worms, new viruses are not identifiable before taking action and hackers have the benefit of testing their malicious creations using commonly distributed anti-viruses and their target`s computers. Newer worms, usually hard to analyse, can easily bypass firewalls and other means of protection, [19] [23]. Hackers can implement new or modify viruses that already exist (there are virus construction kits on the Internet). A substantial number of computers can be infected by a hidden virus that will remain dormant until polling day. It is likely to perform different types of actions, without the elector's knowledge, such as capturing the information needed to log in before it is transmitted to the server and communicating it to a third party, changing the elector's vote before encryption, spy on the elector's vote and disclose it to anyone.

2) Pharming: The elector is the victim of a session hijacking when he has entered the URL of the official website and is navigating using the SSL communications security protocol. He therefore believes that he is polling on the legitimate website when he is actually the victim of a site that merely imitates the real one, including sending confirmation of vote reception. This spoofing can be disclosed if the elector validates a genuine security certificate. However, if a fraudulent security certificate have been accepted on the same computer during at a previous session to a so-called secure site, causing a security alert to be displayed (see Fig 13), which many users usually choose to proceed by clicking on yes, without verifying that they are authorizing a possibly falsified security certificate to join the security certificates properly endorsed by the certification authorities, later log in to the same falsified polling site will not trigger a security alert.

Fig 13: Security alert window

3) Man-of-the-middle: The man in the middle interventions consists of impersonating the server vis-à-vis the elector's computer, and vice versa, the hacker can thus modify the vote that was issued. Vote encryption provide reliable defence against this type of attack if the public encryption key sent to the elector hasn't been hijacked by a hacker. It must therefore be sent to him in a secure mail. On the other hand, encryption key doesn't have to be known to

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

capture the ballot and destroy it, depriving the elector to exercise his voting right, and sending a message back to the elector's post in order to make him believe that his vote was well registered.

4) Denial of service: Denial of service involves bombarding the server with polling requests to prevent legal electors from polling. The server, saturated, cannot respond to all requests and is even likely to break down.

D. Reliability

1) Hardware Errors: Computers may encounter breakdowns or malfunctions. There may be faults in hardware, especially in electronic cards (welds joint failure), or microprocessors. Computers must therefore integrate error detection mechanisms, which might not be carried out systematically on computers owned by individuals.

2) Software errors: Computers might encounter programs errors. Programs' errors can show at all stages: system, software, compilers, security weaknesses, etc., including in a computerized polling system. For this reason, the North American National Institute of Standards and Technology recommends that verification or inspection of the results of a polling system must not be entrusted to a software prone to malfunction [20]. These results have been corroborated by many academic studies on dematerialized polling [11] [18] [19], the Irish Independent Commission on Electronic Polling [2] [3] or international institutions [21]. Several avenues have been searched to identify errors and eradicate them in an Internet polling application: testing, formal program development, expertise, monitoring of election operations and cryptographic verification of results.

3) Tests: Rigorous testing of computer's application does not guarantee its behaviour in future usages, moreover to know its previous function in past uses. It is impossible to reproduce or simulate the stages of a genuine election with tens of thousands of people involved, putting into account all the vulnerabilities that can arise. The testing process, which is generally ineffective to prove a computer's program correction, is even worst with a polling application where malfunctions can go unnoticed due to anonymity.

4) Formal Development: In the field of computer science, to be sure that a program does not contain errors, it is necessary that at least formal techniques of development is exploited. These techniques remain very pricey and restricted to software components. Beyond particular complexities, no safe development techniques are available.

5) Expert Control: Certification authorities do exist but they do not have the capacity to audit programs with reliable means and awareness to discover any security errors and weaknesses. Conclusively, if a review were carried out, even if there were development techniques in place to prevent human pitfalls, there still would be an unresolved problem up till now: ensuring that the programs that have been certified are those in service and are running without alteration contracted by the location (misappropriation of execution by malicious code present in secondary software or microcode driving active components). In any case, servers running an operating system, a code interpreter or a compiler possibly that should also be examined, etc. This approach quickly became monumental and therefore unrealizable.

6) Tracking election operations: To trace how a computer application works, it is necessary to observe its step by step progress. Monitoring programs implementation through software probes raises the question of the neutrality and objectivity of these probes and the programs responsible for analysing observational data. In the context of a polling application, such a follow-up involves the holding of a register in which all events are signed and time-stamped: the arrival of a ballot, the elector's vote, the counting, etc. The problem is that reading this register would disclose all votes, which constitutes a violation of the secrecy of the vote. If the information in the register is incomplete (for the purpose of voting secrecy), then the process turns out to be futile since it no longer allows to follow the processing of the received information and that a malfunction (or fraud), even a major one, can go unnoticed. It is clearly obvious that effective Internet communication measures (such as in banking) cannot be successfully applied because of the very nature of democratic polls which is anonymity.

7) Post-account verification of results: Internet polling is subject to fierce research in the area of cryptography in order to provide standards for any elector to make sure that his vote is well taken into consideration and that the sum of all polls is fair. Electors must also be able to report any evidence of their findings. RIES[15] and VoteBox [22] two highly complex experimental systems are vulnerable to fraud, because complexity is a vulnerability factor: a well-designed cryptographic protocol can be prone to errors and vulnerable to fraud. Even more, if the elector uses these systems for voting and notices an alteration of his vote, he has no opportunity to prove it. Finally, the respect of confidentiality is conditioned by the destruction of intermediate files.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

V. TECHNICAL FLAWS IN HYBRID POOLING

As programmers who wrote the voting program, we could decide that our program actually counts the votes, or we can decide we want this candidate to win and what the program computes, that's a problem. In fact, here's how we can commit election fraud with one of these voting machines

1) you write a computer program that:
   - when it's not being tested that is an on non-election days it has to accurately count the votes in case someone is testing it you know when there's no election going on,
   - but on election day it can add the votes to the wrong column now and we can write cheating programs like this, we have to make sure to wait until at least a hundred votes have been cast before shifting votes around just in case somebody is trying to trick us and test it on election day,
   - voters won't see anything amiss because the user interface will report back to the voter here's who you voted for
   - the pre-election logic and accuracy testing won't see anything amiss because the program is designed not to cheat when it's being tested
2) now the next step is you load our fraudulent program into the voting machine,
   - the easiest opportunity is if you know at the voting machine factory a corrupt employee then we just make all the voting machines cheat
   - but it's easy enough to do it in the field as well in older voting machines, we just have to uncover the machine and replace the memory chip to install our fraudulent program.

On more recent models all we need to do is use the software update process.
So, we should not use touch-screen voting machines this is a fatally flawed technology, fortunately only a few states still use touch-screen voting machines none is being manufactured anymore no company will make touch-screen voting machines because everybody knows that they shouldn't buy any more the only ones left are the ones that stayed still having used and they're too cheap to replace.

VI. EVALUATION

Structuring this assessment is possible through different approaches due to the numerous dimensions that the analysis must make consideration for: observance of the principles that distinguish a democratic vote from any other, the technical principles of each vote's mode, or the time space of election violations. The latter thread will be under scrutiny by addressing the common aspects to the three polling techniques, then individually treating them.

A. Common Aspects of the three Polling Techniques

1) Preparation and Transmission of Polling Materials: An event or wrongdoing may result in not printing (O1) or transmitting (O2) the polling materials necessary to vote to an electorate subset. Mail polling materials may be diverted, lost or postponed during transmission (T1), which may result on electors voting right depravations. This attack on uniqueness and sincerity of the vote may be of average significance, while being of reduced difficulty to an insider. It has an average visibility because, since the mail is not sent with proof of delivery for expense reduction, there is no control over their delivery, electors who are not vigilant might overlook this absence, let alone officially report it. Strict control over the amount of sent letters is vital.

2) Receiving polling materials (V1): Interception of mail once reaching its destination is very possible, from dwellers of the same premise. This fraud is likely to be executed by an individual in the elector's entourage who is generally familiar with the required extra information to be permitted to poll (usually the birth date), but it is of limited scope: a fraudster can only divert a few polls. Biometric processes are sometimes considered to prevent identity theft in the context of Internet polling. This approach encounters different obstacles. First, it opposes several principles of security such that a password must always be stored and encrypted in a single file, and might need to be changed, and the phases of authentication and identification must be distinct. Biometric procedures when implemented are required to use the same data for authentication and identification, whether it is the palm of the hand, the iris of the eye, or fingerprints. This data is susceptible to disclosure and unchangeable. More than that, it has been demonstrated on several occasions the straightforwardness of misleading the biometric systems [17]. Finally, in order to generalize this methodology biometric data of all electors needs centralization to be recognized, which poses essential ethical, organizational and technical problems.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

3) Non-receiving of polling materials (V1): Envelopes that carry polling materials and which could not be distributed are returned to its originating address, i.e. to the organizing centre. It may be tantalizing to use them for voting without the knowledge of its designated recipients. The fraud`s scope is limited by the returned envelopes number to the voting station. The accounting of these envelopes on official minutes is a measure to alert in case of embezzlement in numbers. The extent of this fraud is therefore limited. Expression of Choice (V2) Respect for confidentiality means that the elector polls alone and is not under any pressure. In distant polling in an unrestrained location, none of the postal polling techniques can guarantee that the voter conveys his choice free from pressure. Arrangements aimed at responding to pressure problems and thus increasing confidentiality have been implemented in some Internet polling systems: they give the possibility to poll several times, only the last vote being finally counted13. In addition, electors may be able to poll at the ballot box at a voting station before the official Election Day and cancel their possible Internet polling. Attempts like these will weaken the anonymity`s principle: in order to be annulled, polls must be saved on a server while sustaining the link between the poll and the sender identifier. Introducing multiple polling possibility to eliminate an obvious weakness (at least by the concerned elector) of minor magnitude introduces an obscured vulnerability of major magnitude: the analysis and collection of internal server files can reveal the voters and their expressed choices.

B. Postal Correspondence Polling

Weakest link of postal mailing polling is the polls delivery (T2). Envelopes containing these polls can be hijacked due to their distinct appearance, or can simply fall behind, their non-receiving condition by the centre constitute an infringement on the sincerity of the poll. Even if the postal authorities are supposed to value the letters' secrecy, opening the envelopes can be carried out, in defiance of the polls' confidentiality. Practices for knowing the envelopes 'contents without even opening them can easily be acquired. It would be conceivable to secure postal services by generalizing the utilization of certified mail and inviolable envelopes, but, in addition to the pricey cost of such measures, it seems illusory to extend it to countries where the notion of proof of delivery mail does exist14. Envelopes can be replaced or destroyed once received by the centralizing polling station (O3). These breaches of poll`s sincerity and confidentiality are of average visibility, which amplifies the number of concerned letters. Implementation`s difficulty depends also on the magnitude: effortlessness of taking out two or three envelopes, repeating the operation for hundreds or thousands of times requires many individual's involvement which results on increased visibility. This method of polling was also prohibited for political elections by law following numerous cases of fraud.

C. Hybrid Postal Polling

Hybrid mail polling has the same weaknesses as postal mailing polling with respect to postal delivery of polls (T2). Similarly, polling envelopes and its contents can be destroyed or stolen after reaching their destination (O3). Replacing polling envelopes and its contents is much more difficult than for postal polling because the uniqueness of each polling card. The extent of such fraud may therefore be reduced if the process of making polling cards is isolated from the centralizing polling station. The counting stage (O4) is automated. The polling cards with each elector's ID and choice are stripped by a single software that manages both the list of vote updates and the vote count. The separation between polls, identifiers and elector identities is not clearly established. The unveiling of the electors' vote is within the reach of those with access to the software that performs the counts or the data. This breach of polling secrecy can be carried out by only one person which may result on affecting all polls while staying obscured.

D. Internet polling

1) Preparation and transmission of polling materials: Identifiers and passwords in electronic form can be copied during their generation, or at the printer responsible for the production of letters (O1). This manoeuvre may affect all electors and does not pose significant complexities, while remaining obscured. However, to enhance security, additional information, such place or date of birth, is often requested. Collecting this type of information can be an overwhelming task if the number of people involved is large, limiting the information volume needed to vote. In order to eliminate this stage, and thus the weaknesses that goes with it, it might be possible to provide each elector with an identifier in the form of an electronic card. Oddly, this solution results on a risk substituting another: the utilization of a single electronic identity card to carry out various transactions (polling, paying taxes, etc.) makes citizens vulnerable to the abusive procedures of a country that might be tantalized to cross-reference these data. This

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 2 , February 2020

significant risk should not be ignored, since a country tantalized to do these sorts of practices certainly wouldn't be willing to bring it up to the public [10].

2) From the Expression of Choice (V2) to the Receipt of Polling (O3): These steps result in interactions between the elector and the official polling site server. A virus on the computer used to poll can capture the poll between the validation phase (V2) and its encryption (V3) and transfer it to 3rd parties, or implement a session hijacking capturing the elector's information. Captured information such this can be abused by polling without the legitimate elector consent. Likely to affect considerable number of polls, these actions can remain almost obscured. Their realization does not present any actual difficulty for a determined computer expert. On the other hand, the denial of service, which has the principle of disrupting access to the polling site, is immediately visible. Then again, many employees might be forced to poll from a workplace computer, particularly if this poll relates to their jobs, without always realizing that organization are exercising increasingly tight control and that they would therefore be able to spy on the polls of their employees.

3) Reception (O3) and Counts (O4): In any Internet polling app, each ballot travel accompanied by the elector's identity. This information arrives together on a first polling server. This is exceptionally delicate and has been the subject of many publications related to polls encryption and how to be implemented in such a way where the elector's identity can be decoded regardless of his vote ([12] for example), but polls reconstruction is still achievable from Intermediate files stored in the server with received information, even through encryption (having sufficient time and data to investigate it are factors that simplify this sort of fraud); technical measures cannot be put in place to make it impossible for an individual with malicious intentions and access to servers to violate the poll's secrecy. There are classic fraud processes such as a back door or a Trojan horse. These frauds boil down to the insertion of a limited number of lines that can certainly go undetected in the midst of programs with several thousand lines [19]. These malfeasances can be set up by only one person, whom could be an updates and maintenance technician, a programmer, or anyone with logical or physical servers' access. The fraudulent program can change up to all polls received. Finally, the combined automation of the updating of signature registers and the dematerialization of ballots facilitates large-scale ballot stuffing: a fraudulent program can generate the polls of many electors absent in the final moments of the polling period. This risk cannot be controlled by monitoring turnout (it has been observed that polling stations experience attendance peaks in the final moments of election closure). Stopping it by checking electors is not possible: even if an elector realize that a poll has been transmitted in his/her name, in spite of not polling, proving it is considered impossible.

VII. OUTCOME

A. Synthesis

None of the postal polling systems reviewed can be described as safe. But weaknesses can have heterogeneous consequences.

1) Postal Correspondence Vote: is susceptible to fraud and largely dependent on postal services, but these breaches of election sincerity cannot go unseen when they are large-scale.

2) Hybrid postal polling: if it exclusively entrusts vote and vote counts to automatic process, then it will prevent any external intervention on this decisive stage of a vote. The counting process may be the site of a large-scale malfunction or fraud that keeps the totalled polls intact but weakens its authenticity. Establishing such fraud would demand hand-stripping of all the ballots received, which is not possible with thousand ballots due to practical difficulties (the ballots must be kept under seal, sufficient people to achieve counting, enough time and, more than that ability to explain the need for such an operation) and legality (recount not carried out, no physical evidence will be available to support the suspicions to be presented to the qualified election judge to order this new count). Polling software can disclose electors' choices to third parties without this breach of polling secrecy being proven. This process, which appeared without any genuine reflection beforehand, shows important and obscured weaknesses in respect for sincerity and confidentiality.

3) Internet polling: Worst case situation in Internet polling reveals multiple weaknesses: obscurity that can affect many polls; fraud which doesn't require expensive equipment can be committed by a handful of people. These weaknesses appear at different phases of the polling process: in the elector's home, when polls are being delivered, or at the time of counting.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 2 , February 2020

B. Analysis

Examined weaknesses of the techniques used in distant polling affect polling stages that are beyond the direct scrutiny of polling controllers, scrutineers, delegates and candidates' representatives. Stages such these are susceptible to corruption without everyone's knowledge. With traditional postal mailing polling, areas of imperviousness are limited at the time of the elector's vote and the transmission of mail. Automatic hybrid vote counting expands the areas of imperviousness by hindering public counting of polls during counting. Internet polling radicalizes this process of automation by manipulating only dematerialized objects. The polling process is thus moved from the genuine world, whose experience is palpable by the public majority to a virtual realm where theirs perceptions (touch, sight, etc.) do not apply. Directly monitoring the polling process and assess the extent to which it is proceeding properly is almost impossible. We simply have to look at processes that are expected to manifest the polling system activity, which can also provide a misleading representation of it. Polling operations are then at the mercy of events that may remain obscured: criminal acts (simpler to commit as the proximity from the election organizational team is large) or even simple malfunctions. It finally appears that information technology is helpless in the face of this problem. Writing a large program with no more errors is considered an achievement. However, ensuring that a program does not host any deliberately concealed "mistakes" is a much more complex task. Neither the tests nor the program expertise is sufficient. It is impossible to protect a program from being injected with untrusted code no matter how long its code has been systematically scrutinized and verified. Lower level of coding means harder bugs to detect. A microcode bug cleverly installed will be practically impossible to discover. [19]

VIII. CONCLUSION

This study presented the weaknesses of three technical forms of distant polling when it is used toward establishing democracy in Middle Eastern Countries. It has shown that the utilization of computer tools, accompanied by the intensification and complexity of internal process, makes the democratic polling process vulnerable to massive attacks on the sincerity of the results or respect for privacy. It appears that the dematerialization and conversion of information inherited in any computer processing plunges the polling process into a new universe where the rules of ordinary physics no longer apply. The impossible becomes possible (modifying thousands of polls in an instant). For example, in the reality the simple shuffling of postal polling envelopes definitively eliminates the links between polls and electors. In the virtual world, there is no way to always achieve this without fail: files may have been copied, information improperly erased, etc. In Tunisia the Ministry of Communications and Information Technology demands independent management of signatures and polls but looks oblivious to the fact that this separation will not prohibit breaches of polls' secrecy. The EU which usually deploy an Election Observation Mission (EOM) for the presidential elections in Arab countries describes transparency as availability of an option to verify the correct functioning of the polling system, which is technically impossible with what has been previously established. Or it advises that an elector should be able to acquire a successful poll commit confirmation and/or correct it when this possibility can result on a trace back or establishing a connection between the poll and the elector, thus weakening anonymity secrecy. These stammering efforts to safe guard anonymity, provide polling protection, and dematerialize polling elements confirm that this move to electronic polling poses original, particular problems, and reveal surprising contradictions and resistances.

So if we shouldn't vote on the internet how should we vote in the 21st century, well if we go back to the voting protocol previously mentioned we have an optical scan ballot where the electors fill in the bubbles then feed it to the scanner, we put that scanner in place of the ballot box in the election site so we preserve voter registration integrity even in the presence of untrusted parties or poll workers, we preserve the secret ballot in a way that we know who's not shoulder surfing over us because it's in a neat space that we understand. Where different parties' representatives watching the ballot box, are going to watch which optical scan form gets fed into which optical scan counter. That protocol works pretty well except that optical scan machine is a computer it's got software that programmers decides how it's going to add up those votes, what's it going to report, which is a problem, but there's a solution for this problem. The paper ballot which is actually marked by the voter without any computer user interface interpreting it to him or her is fed into the optical scan counter and drops into a ballot box and now at the end of the election day you've got a sealed ballot box with a vote with the ballot actually marked by the voters and you can recount them by hand without any computer interpreting them to us as a check up on the possibly fraudulent software in the optical scan machine. Now, if we have to recount of ballots by hand then why do we bother with the optical scan machine well, first of all it is quite accurate and fast when it hasn't been hacked so we get our results immediately that is the polls close, but also if enough different optical scan ballot boxes have been hacked, that it can influence the results of a big election, we can't just simply hack

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 2 , February 2020

one optical scan ballot machine, we have to hack a whole bunch, so if you take a random sample of those ballot boxes and recount the paper ballot by hand to match up the results to what the optical scan machines reported then statistically you can detect fraud if it's widespread enough to make a difference. In fact, almost all of the states use optical scan voting which is a good thing in about half the states have these audit practices are encoded into law that you conduct a you recount a random sample of the optical scan and balance. So that's how we should vote in the 21st century and pretty much that's how we do vote it's not perfect but it's good enough. So, where does that leave us, are we willing to outsource counting our votes to whoever happened to install the software in the server and in our client machine even if we trust that person to be honest do we trust that person to design a server and a client machine that is so secure that the hacker can't go in there and replace vote counting software, that's an extremely high level of trust and events in the real world do not lead us to make that level of trust.

REFERENCES

[1] BIRDSALL (S.) The democratic divide, first Monday, peer-reviewed journal on the internet, (2005).
[2] CEV. Commission on Electronic Voting, Secrecy, Accuracy and Testing of the Chosen Electronic System", first report, (December 2004).
[3] CEV. Commission on Electronic voting. Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. second report, (July 2006).
[4] Kermmis S., "Action Research," in Hammersley M. (Ed), Educational Research – Current Issues, Open University Press, vol. 1, 1993.
[5] COLEMAN (S.) "Internet voting and democratic politics in an age of crisis". in Trechsel A. (ed.) The European Union and E-Voting: Addressing the European Parliament's Internet Voting Challenge, Londres: Routledge, p.223-237, (2005)
[6] Krutchen P., "The 4+1 View Model of Architecture," *IEEE Software*, vol. 12, no. 6, 1995.
[7] Kolb D. A., Experiential Learning: Experience as the source of learning and development, Prentice-Hall, New Jersey, 1984.
[8] Newble D., and Cannon R., A Handbook for Teachers in Universities and Colleges, Kogan Page, 1991.
[9] Ramsden P., Learning to Teach in Higher Education, Routledge, London, 1992.
[10] DESWARTE (Y.), MALCHOR (C. A.) *Current and future privacy enhancing technologies for the Internet*. Ann. Télécommun., 61, n°3-4, p.399-417, (2005).
[11] DILL (D.), DOHERTY (W.) *Electronic Voting Systems. Report for the National Research Council*, (November 22, 2004).
[12] GÓMEZ OLIVA (A.), SÁNCHEZ GARCIA (S.), PÉREZ BELLEBONI (E.) *Contributions to traditional electronic systems in order to reinforce citizen confidence*. Electronic Voting 2006, 2nd International Workshop, GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), p.39-49, Bregenz, Austria, (August, 2nd-4th 2006).
[13] HERRNSON (P. S.), NIEMI (R. G.), HANMER (M. J.), BEDERSON (B. B.), CONRAD (F. G.), TRAUGOTT (M.) *The Importance of Usability Testing of Voting Systems*. Electronic Voting Technology Workshop, Vancouver B.C., Canada, August 1, 2006.
[14] HOFF (J.) *Towards a theory of Democracy for the information age*. Discussion paper for the Democracy Platform UK-Nordic Meeting, (16-17 September 1999).
[15] HUBBERS (E.), JACOBS (B.), PIETERS (W.) RIES - *Internet Voting in Action*. In R. Bilof, Proceedings of the 29th Annual International Computer Software and Applications Conference, COMPSAC'05, pages 417-424. IEEE Computer Society, (July 26-28, 2005).
[16] SCHNEIER (B.) "The Trojan Horse Race. Inside Risks 111", Communications of the ACM, vol.42, n°9, (September ج1999).
[17] SIFAKIS (J.) cited in "In Search of Dependable Design" by Leah Hoffman. Communications of the ACM, vol.51, n°7, p.14- 16, (July 2008).
[18] MERCURI (R.) "A Better Ballot Box?" *IEEE Spectrum Online*, (October 2002).
[19] SIMONS (B.) "Electronic Voting Systems: The Good, the Bad, and the Stupid." ACM Queue vol.2, no.7, (October 2004).
[20] THOMPSON (K.) "Reflections on Trusting Trust". Communication of the ACM, vol.27, n°8, p.761-763, (August 1984).
[21] OSCE/ODIHR. USA 2 November 2004 Elections - OSCE/ODIHR Needs Assessment Mission Report. 7-10 September 2004, Warsaw, (28 September 2004).