Internet-Voting: Opportunity or Threat for Democracy?

Emmanuel Benoist, Bernhard Anrig and David-Olivier Jaquet-Chiffelle

V.I.P. - Virtual Identity, Privacy and Security
University of Applied Sciences Bern – Quellgasse 21, CH-2501 Biel

Abstract During the last decade, Internet-voting (i-voting) moved from the field of fundamental research to practical application. First, we will see that theoretical research provides satisfying algorithms for some of the challenges raised by i-voting and that some real world experiments have already been developed and performed.
Unfortunately, in current i-voting systems, the citizen loses his/her control over the overall electoral process. Indeed, only insiders usually have access to the programming code of the application and to the servers used in i-voting. The confidence in democracy itself could be harmed by this opacity.
The European Convention on Human Rights emphasizes that votes should remain secret. This can not be assured for i-voting, since it is not possible to have a booth around each computer for example during the voting process. Family voting cannot be prevented and vote buying could be a major threat for democracy.
Moreover, we can not assume that the voter's computer contains no viruses or Trojan horses. Therefore, it is optimistic to assume that the ballot transfered to the server is the one chosen by the voter.
Finally, we will see that the effect of i-voting on the turnout at polls might remain marginal. E-Voting, Internet, Democracy, Recommendation, Citizen empowerment

1 Introduction

For many researchers in the area of computer security, i-voting is a very challenging and motivating topic. We observe also a growing interest from administrations as i-voting is expected to increase the number of voters while saving money during the counting of the ballots. We will see that i-voting will soon become a reality, but that it will also imply some change in the citizen's empowerment for the whole voting process.

In most developed countries, the rate of people choosing to vote has dropped drastically over the last decades. For instance in the general election in Switzerland the turnout at the polls has constantly decreased during the last century passing form 80 percents in 1919 to 45 percents in 2003 [?]. The same process is visible in all Western countries where voting is not mandatory. Politicians think that the voting process has to be modernized and that it would have a major impact on the turnover. Since Internet is now used extensively by a large proportion of the population for e-banking, e-tickets for airlines or train, etc. the government should offer the same type of service for voting also. They want to offer a way to vote that is as close as possible to the way people live [?].

The penetration rate of cell phones is far above the one of Internet, that is the reason why the administration of the Canton of Zurich in Switzerland even wants to organize e-voting using cell phones. Such a system has already been tested for the election of students representatives at the University of Zurich [?]. The same system has also been tested on a small scale for real votes (also in the Canton of Zurich).

Moreover, organizing elections costs a lot of money. It is tempting to use new technologies in order to reduce the costs. Private industry uses Information Technologies to increase productivity; why should the administration not use new e-voting technologies, like i-voting, to gain productivity and save money? This argument is particularly relevant in a direct democracy such as Switzerland for example, where voters have to cast a ballot typically four times a year and where each ballot paper contains several questions (local, cantonal and/or federal ones). The traditional handling of the ballots — i.e. counting by hand — is expensive and time-consuming. This explains why some administrations are in favor of i-voting, hoping to save time and money. Last but not least, i-voting carries also the positive image of a modern technology.

2 Encouraging Results

In the last decade, several encouraging results have been found in the area of i-voting. First, researchers from the area of computer science security have developed protocols to ensure a secure voting process. Then some countries (or regions) have developed and introduced i-voting at a larger — but still limited — scale, proving its feasibility: this was for example the case in Geneva, Neuchâtel and Zurich in Switzerland [?,?,?].

Many publications have been written presenting i-voting schemes. Most of them respect the following golden rules of i-voting presented by Cranor and Cytron [?]:

- **Accuracy**
  - A cast vote can not be altered.
  - An invalid vote is not counted.
  - Each voter has the guarantee that his/her ballot is counted.
- **Democracy**
  - Only an authorized voter can participate.
  - Each voter can cast only one vote.
- **Privacy**
  A ballot can not be linked back to the voter who cast it.
- **Verifiability**
  Each voter can verify that his/her vote is counted.

Ray et al. [**?**] defined an additional rule: **No Unauthorized Proxy**. If a voter decides not to cast his/her ballot, no third party can take advantage of this and cast a forged ballot.

It is possible to design a voting protocol fulfilling all those requirements. Most of the algorithms [**?**,**?**,**?**] use anonymous channels to cast the ballot as an untraceable message. Ray et al. developed an algorithm using very soft cryptography; voting is done in five phases:

1. Blank ballot distribution: the voter identifies himself/herself with his/her certificate and gets a blank ballot.
2. Generating a voter mark: the voter generates a mark from this ballot.
3. Voter certification: the voter gets a blind signature on his/her voter mark.
4. Vote casting: the voter transfers the signed voter mark together with its ballot to the server.
5. Vote counting: once the voting period is over, all cast ballots are made public and the results are announced.

Some countries have already introduced i-voting on a significant scale. For instance, a few Swiss cantons have implemented i-voting schemes and are testing them already in real votes. The main principle (for the Canton of Geneva) is simple. Each voter receives a voting card containing a field that can be scratched off. This field contains a one-time secret password for the voter. The voter connects to a dedicated server, gives the secret number and can enter his/her ballot using a website accessed by the `https` protocol[1]. Actually the i-voting implementations of the three Swiss cantons differ. Some implementations seem to be more mature and secure than others.

The three cantons mentioned above have already organized votes with e-voting where the citizens have participated in real elections or voting. The Canton of Geneva has developed an Internet platform for i-voting. The system is dedicated to i-voting only. Additionally, this canton is already planning to introduce i-voting on a larger scale and a new law i.e. a modification of the constitution, is almost ready and should soon be presented to the cantonal parliament [2]. In the Canton of Neuchâtel, i-voting is part of the general e-government portal "Guichet Unique" (GU). Citizens can not only vote using this system, they can also fill in their tax declaration on-line, follow up the tax invoices and tax payment. Not all citizens have a GU account; among the ones who have, around 54% percent voted using GU. The tests in the Canton of Zurich were using two different e-voting platforms: Internet and SMS. For SMS, the voter does not send his/her choice in clear text form (for instance "Yes" or "No"). He or she receives a table containing a code for each possible choice, then the voter sends the code corresponding to his/her choice to the SMS gateway. The votes are anonymized afterward and transfered to an electronic voting box. This test has also been a success; it has been used for the election of the board of students at

[1] `https` is a combination of a normal `http` over a Secure Sockets Layer SSL or Transport Layer Security TLS.

[2] Proposition de loi 9931 et proposition de loi constitutionelle 10013

the University of Zurich. During this election, only one student did vote using a paper ballot, all others used e-voting, i.e. 1582 using Internet and 205 using SMS. Even for a real election (Bülach April 2006), 20.67% of the voters used e-voting, among which 3.85% used SMS voting [**?**].

It is interesting to point out the significant difference between the complexity of academic crypto-solutions, that are proved to be secure under certain assumptions, and the simplicity of the techniques chosen in current real life implementations. But we have to keep in mind that the requirements are not the same for both cases. In academic research, i-voting is a goal in itself and both security and trustworthiness are top priorities. In real life, one has to try and fulfill new practical constraints that might be incompatible with some secure academic solutions. Indeed, i-voting is currently introduced to make the voting process easier and more attractive, in order to gain new voters. Therefore,

- it should **be very simple and easy to use**: i-voting is intended to be used by many voters; even older or disabled people should have the opportunity to use it,
- it should **not require any special installation**: it should be based on open protocols (`http/https/ftp`), and should not require any specific client software,
- it should **be compatible with other off-line voting mechanism**, since we probably won't and cannot force all citizens to do i-voting.

These three added constraints explain partly the gap between theoretical results and current practical solutions.

3 Empowering the Citizens?

One of the goals of politicians supporting i-voting is to increase the number of voting persons, and hence improve the democracy. Yet the outcome might be paradoxical, since in many points, introducing i-voting could reduce the power of the citizen and its confidence in the voting process itself and consequently harm the democracy.

In traditional voting processes, citizen usually can verify, either directly or indirectly, the way their ballot has been taken into account.[3] They typically put their ballot in a special box, and can assist later to the counting of the ballots. In the countries where citizen cannot assist, it is possible to have people monitoring this process. Everybody can convince himself/herself that each vote has been counted correctly.

This type of confidence in the system should be saved for i-voting. Administrations have to provide at least the same level of confidence. Some algorithms, such as the one of Ray et al. [**?**] provide a way for the voter to check if his/her vote

[3] There are famous exceptions like the "Landsgemeinde" in Switzerland where votes are expressed by raising one's hand and are visually counted by trusted experts.

has been taken into account. But, the voter must also be convinced that the program used for the i-voting is really working as it is supposed to be. That means, in particular, that it fulfills all the requirements seen above. Unfortunately, in the domain of i-voting, security by obscurity is often the rule. A "normal" citizen can neither access the code, nor see the type of algorithm used, nor check that the machine is well configured and that the administration or other third parties do not manipulate votes. In traditional voting processes, forging 100 ballots is nearly 100 times more difficult than forging one ballot. This difference does not exist in i-voting, since the fraud can be reproduced almost without extra costs. Manipulating ballots at a large scale seems to be easier and less detectable in i-voting than in traditional voting.

In order to give citizens more confidence in the system, we need a totally transparent i-voting process letting the citizen monitor each of the steps. Confidence in the democratic process can only be reached when i-voting uses transparent boxes. That means that any citizen should be able to access the algorithm, and read the code. In particular, only Open-Source projects should be accepted for i-voting. But this would not be sufficient. Citizens must be able to check if the program they inspected is really the one that is running on the server. There is unfortunately no way to achieve this goal. One can nevertheless try to certify what happens on a server. Trusted computer can for instance certify that the boot-process used by the server was right. It is also possible to use a micro kernel that can be totally verified on such a trusted computer. Unfortunately, such systems are not secure enough and can not be used in a productive environment.

4 Can Voting Remain Secret?

In a traditional voting process, voters are hidden in polling booths while filling in their ballot. There is no such booth in current i-voting systems. Family voting cannot be prevented and vote buying could become a major threat for democracy.

The article 3 of the Protocol 1 of the European Convention on Human Rights says: *"The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature."* [**?**]. This protocol has been signed and ratified by almost all the European countries (except Switzerland). It means that ballots have to be secret; nobody should be able to know who voted for which candidate. With i-voting, one can verify the way a voter votes by forcing him/her to vote under surveillance. Or someone can get the empty voting cards of all his/her clients and can vote for all of them. This can be used for vote buying. There are ways to circumvent this by adding a secret key. If the key is false when voting, then this vote is not counted but both the user and the observer do not see it. However, i-voting becomes more complicated and the risk of an error in such a manipulation is high. The voter cannot see that his/her vote is not valid, he/she might lose his/her possibility to cast a ballot for this election.

The second risk is family voting. The Venice commission of the council of Europe has produced a Code of Good Practice in Electoral Matters [**?**]. In its article 4 about secret suffrage, it says that *"secrecy of voting is not only a right but also a duty, non-compliance with which must be punishable by disqualification of any ballot paper whose content is disclosed"*. It is also said, that *"Voting must be individual. Family voting and any other form of control by one voter over the vote of another must be prohibited"*. That is the reason why they express huge concerns about postal voting. For the council of Europe, it should not be widely encouraged and should be reserved for special cases. *"Postal voting can be used to enable hospital patients, persons in custody, persons with restricted mobility and electors resident abroad to vote, in so far as there is no risk of fraud or intimidation."* These restrictions should also be extended to i-voting, since it is not possible to physically ensure the secrecy of the votes. There is no way to check if a voter voted free or under control of another family member.

Moreover, even when the transmission over the Internet might be well protected, there is almost no protection of the voters' computers. It is not reasonable to expect for a "normal" user to protect its screen with a Faraday cage in order to not be spied on . . . It it not reasonable to expect that computers are virus free, or that they do not contain any Trojan horse. A fundamental security weakness of i-voting is on the side of the voters which use their own machines.

Rubin [**?**] presented a study of the security weaknesses for i-voting. One can start with the server that could be controlled by an attacker. The network can also be attacked (Distributed Denial of Service attack for instance). But the major risks are situated in the voter's computer. Some possible attacks may consist in taking the control of the computer, modifying the browser or the operating system, in such a way that the vote transmitted by the computer is different than the vote the voter has chosen. The attacker would manipulate Input and Output so that the voter would not see any problem and would have the feeling everything was right. It is also possible to use a key logger, in order to monitor the way people vote. Since operating systems and programs used on the server and on the client contain typically many thousand lines of code, failures are contained therein. It is not possible to formally verify each piece of code [**?**,**?**]. Those failures can (and will) be used by hackers to access the system. Security measures can be taken, but zero risk is impossible to be reached nowadays. Since attackers may be states (a foreign state or even the state organizing the vote), there is potentially no limit to the power of the attackers.

In order to control the result of a tight vote, attackers don't need to take control of all the computers of the voters. For a tight election, say 51% to 49%, controlling only 3% of the votes would allow to change the result of the election. Since the 3% are unknown, only half is changed from the former winner to the former loser (the other half of the votes are already destinated for the former loser) so 1.5% is transfered, which makes the result changing from 49.5% to 50.5%.

5 Is It Worth the Price?

One of the goals for governments to use i-voting is to increase the proportion of people that are voting. It is difficult to assess if i-voting is a long term solution to motivate people to vote. However, we can already study the effects of the generalization of postal voting on the turnout in Switzerland. Almost all Swiss Cantons have generalized the postal voting in the middle of the 90's (and already the late 70's for some cantons). In these cantons, any citizen receives one ballot that can either be used for traditional voting or postal voting. We can see in Fig. **??** that the number of voting citizens has not significantly increased since the middle of the 90's. At least it stopped decreasing [**?**,**?**]. Two studies have been conducted in Switzerland: a team of the University of Geneva (c2d – centre d'étude et de documentation de la démocratie directe) estimates the potential of gain to be 9% whereas study of Hanspeter Kriesi from the University of Zurich estimates the gain to be at most 1.7%. [**?**]

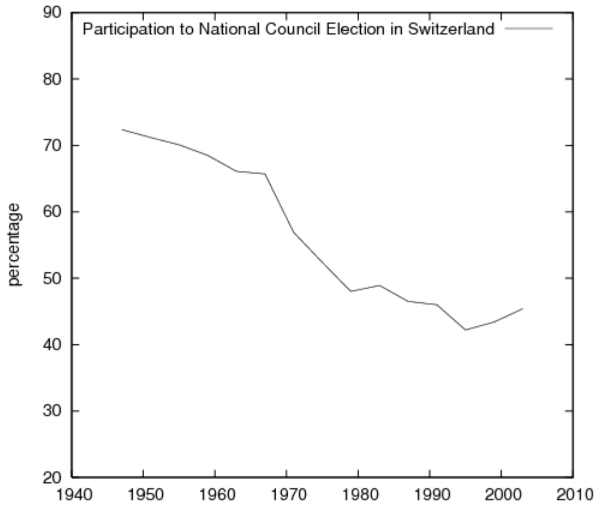

Figure1. Voters for the General Elections in Switzerland (1995: generalization of postal voting)

As we see, the effect of the generalization of postal voting in Switzerland has been positive, but limited. Nevertheless, in Switzerland, it is widely accepted that the added value of postal voting, in terms of convenience, is worth the price in terms of security: making easier family voting.

However, it is questionable to assume that the added value of i-voting, in term of convenience and in comparison to postal voting, is worth the extra risks (vote buying, large scale frauds, loss of the citizens' confidence in a fundamental democratic process, etc.) brought by current implementations. In countries where postal voting is not implemented, we could expect the introduction of i-voting to have an impact similar to postal voting in Switzerland as it brings a similar added value in terms of convenience. As we see, this impact — though positive — might remain marginal.

Current i-voting experiments (mis)use the confidence that people have in traditional democratic processes with a long successful history. Any abuse of this confidence might be very counterproductive in the long run. What will the impact on the proportion of voters be, when citizens realize that they have lost most of their control on the voting process? Citizens may even lose confidence in the whole democratic system, since they can not be sure about the way people are elected or decisions are taken.

We recommend that governments and administrations be very careful with the introduction of i-voting and apply the precautionary principle. If an i-voting system can fulfill all the requirements presented in this paper (securely proven algorithms, simple implementation, open-source program, and transparent computer) and its use is limited to absentee voting (hospital patients, persons in custody, persons with restricted mobility and electors resident abroad to vote), then i-voting could become a successful application of a new technology. As for today, there is no way to have a transparent server, since clients are still totally insecure, it is premature to introduce i-voting and administrations should wait before deploying such a system. Otherwise, it might as well reveal itself as major threat for democracy.

References

1. Swiss Federal Parliament (National Concil): Turnout at the polls from 1919 to 2003. http://www.parlament.ch/e/homepage/wa-statistiken-diagramme/wa-statistiken-diagramme-wahlbeteiligung-ab-1919.htm
2. Hensler, R.: Les nouvelles technologies, ferment de la modernisation de l'etat. In: 5e symposium suisse eGovernement, Swissôtel Zurich-Oerlikon (2004) http://www.geneve.ch/evoting/discours_20040826.asp.
3. Statistiches Amt des Kantons Zürich: Abgeschlossenes pilotprojekt e-voting des kantons zürich. http://www.statistik.zh.ch/produkte/evoting/index.php?p=5
4. Canton de Genève: Site de l'état de Genève consacré au vote par internet. http://www.geneve.ch/evoting/
5. Canton et République de Neuchâtel: E-democratie. http://neuchatel.ne.ch/profils/politique.asp/1-11-160-12345-5001-1001-1-1-2-1/2-0-2345-5001-1000-2-0/
6. Cranor, L.F., Cytron, R.K.: Design and implementation of a practical security-conscious electronic polling system. Technical report (March 25 1996)
7. Ray, I., Ray, I., Narasimhamurthi, N.: An anonymous electronic voting protocol for voting over the internet (November 26 2001)
8. Boyd, C.: A new multiple key cipher and an improved voting scheme. In: Advances in Cryptology – EUROCRYPT '89. (1989) 617–625

9. Chaum: Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In: EUROCRYPT: Advances in Cryptology: Proceedings of EUROCRYPT. (1988)
10. Juang, Lei: A secure and practical electronic voting scheme for real world environments. TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems (1997)
11. Swiss Federal Chancellery: Rapport sur les projets pilotes en matière de vote électronique. `http://www.admin.ch/ch/f/ff/2006/5205.pdf` (May 2006)
12. European Court of Human Rights: European convention on human rights and additional protocols. Registry of European Court of Human Rights (September 2003) `http://www.echr.coe.int/echr/`.
13. Council of Europe - Venice Commission: Code of good practice in electoral matters (July 2002) `http://www.ohchr.org/english/law/compilation_democracy/docs/compil_democracy.pdf` p118.
14. Rubin, A.D.: Security considerations for remote electronic voting. Commun. ACM **45**(12) (2002) 39–44
15. Hoglund, G., McGraw, G.: Exploiting software: how to break code. Addison-Wesley, pub-AW:adr (2004)
16. McGraw, G.: Software security: building security in. Addison-Wesley software security series. Addison-Wesley, pub-AW:adr (2006)
17. Swiss Federal Chancellery: Enquête sur le vote par correspondance. `http://www.admin.ch/ch/f/pore/va/doku/pdf/enquete_bsa.pdf` (1999)