iVote.lt - a practical attempt to overcome online voting - related fears

Jonas Udris
Election Law Expert
Vilnius, Lithuania
jonas@sutartys.lt

Abstract - The paper presents the first practical attempt to introduce the advantages of online voting to the general public, offering a fully functional prototype that covers every major aspect of the online voting procedure. The authors believe that the success of this project will ease the fears and remove the doubts related to the introduction of online voting in binding elections.

Keywords—online voting, Lithuania, ivote.lt, simulator

I. THE SHORT OVERVIEW

iVote.lt is the first Lithuanian online voting simulator, which was aimed to promote and popularize online voting. The project took place prior to the official Parliamentary elections of 2012 and was hosted by www.delfi.lt, the largest Lithuanian online news portal. A total of 3566 people tested iVote.lt, which is three times as many needed for a sociological survey. More than 30 000 people at least tried the simulator; i.e., they have read the description, viewed the presentation, and downloaded the simulator software. This is more than number of voters required for one constituency. Ninety-eight percent of participants of the project voted "Yes" for introducing online voting in Lithuania.

II. INTRODUCTION

First attempts to introduce online voting in Lithuania took place in 2005, when the Concept (Draft Law) on Internet Voting was prepared by the Central Electoral Commission (CEC) and presented to Parliament [1]. Since then, multiple initiatives aimed to introduce online voting did not pass the submission stage in Parliament. Those initiatives were supported in many public, academic, and political discussions, but none led to any tangible results.

Despite the technological progress of Lithuania - where Internet speeds are among the fastest in the world, Wi-Fi hotspots grow like mushrooms in the forest after the rain, people no longer go the Tax Inspectorate in person, and banks close their offices due to the lack of visitors - online voting is still far beyond the horizon. Politicians and some part of the public believe in urban myths like "every computer system is hackable", and that online voting would lead straight to widespread electoral fraud.

To scatter these myths and increase public confidence in the idea of voting online, encourage politicians to overcome their fears, and introduce this modern way of voting, this fully-functional online voting simulator was created and introduced to the Lithuanian public in September 2012, four weeks before actual parliamentary elections. It was called the "iVote.lt project".

The goal of this paper is to present the iVote.lt project and explain how it helped increase public confidence in online voting.

III. THE IDEA

The idea was to put together the knowledge of CEC officials, the power of popular online media, and the capability of a team of programmers in order to present a working simulator that demonstrated and allowed people to try this new way of casting their vote. The simulation game invited people to try the online voting and help resolve all the myths and doubts that surrounded this way of casting a vote in real elections and referendums of the future.

The simulator had to demonstrate that online voting could be a secure and reliable voting method that fully complies with the democratic election principles set in the Constitution, the election laws, and international standards of free and democratic elections. Among those principles are the following: Free elections, Secret voting, Equal voting rights, Audibility, Reliability, Flexibility, Uniqueness, Integrity, and Convenience [2].

The project was started in January of 2012 by online voting enthusiast CEC member Jonas Udris and online media producer Justinas Vanagas. They defined the scope and aim of the project. A private IT company, UAB "EVP International", which specializes in creating online payment systems, was invited to join the project. The owner, Mr. Kostas Noreika, kindly agreed to help and appointed a team of programmers to code the software of the simulator.

The Central Electoral Commission, the Minister of Transport and Communications, and the Minister of Justice expressed their moral support for the project, and the State Enterprise Center of Registers kindly allowed the project to use their online identification system, www.ipasas.lt.

Technically, ivote.lt was based on early versions of the Estonian online voting model [3]. During the design phase many legal, information technology and election specialists contributed their knowledge and expertise to the project. The authors also tried to follow to the Recommendation Rec(2004)11 of the Committee of Ministers to member states

on legal, operational, and technical standards for e-voting [4].

The project followed exclusively informational and educational objectives. It was not part of any election campaign and did not mean to promote any political party or power. The people behind the project were not politically biased and did not belong to any political power. The project had no aim to influence election results in any way.

The simulator was not designed to imitate the real upcoming elections of 2012 or to predict their outcome. It was designed to motivate the society to show their interest in online voting as an alternative way of casting a vote.

The results of the game were completely anonymous; therefore, personal political preferences of the participants were not made public. Some statistical information was presented as additional information, such as the distribution of the voters by age, gender, and geography.

IV. The Design

The main idea behind the iVote.lt project was the "double envelope" voting principle, which is basically a digital version of traditional advanced voting by post. The voting process consisted of five major steps: 1) Generating a pair of keys; 2) Filling the ballot and encryption; 3) Casting the ballot; 4) Anonymisation; 5) Decryption and tabulation of the results.

The simulation game was designed following the principles of transparency and auditability. Therefore, only well-known and open-source libraries were used:

- The www.ivote.lt website was created using open source Symfony2 carcasus; HTTPS protocol was used.
- www.ipasas.lt of State Enterprise Center of Registers was used for user authentication.
- Java Web Start application (JRE 1.5 version and up). The source code signed by Code Signing certificate.
- Bouncy Castle Crypto (http://www.bouncycastle.org/java.html) API was used to encrypt the ballot. Data was then put to a CMS Enveloped Data package and encrypted with a 128 bit key.

The source code of the project was open for public download.

A. Generating the pair of keys

First, the pair of digital keys was generated. The Public Key was uploaded into the system and the Private Key was deconstructed and put away for safekeeping until the end of the voting. Parts of the Private Key were burned onto blank CD's and distributed among organizers of the simulator.

B. Filling in the ballot

The voting simulator was accessible either directly at www.ivote.lt or via the news portal www.delfi.lt, where it was widely advertised. The user was offered the download of a small JAVA applet, which contained an electronic "ballot" and a questionnaire, together with an encrypting algorithm and a Public Key. There was no need for any specific IT knowledge or software installation to use the simulator. The simulator worked on all JAVA-supporting operating systems, including Windows XP and higher and Mac OS X version 10.6 and higher.

Once the user finished "filling in the ballot" and the questionnaire, he or she was then asked to click a button that read "Encrypt the ballot". After the encryption was complete, the binary file containing encrypted information was generated and saved onto the user's desktop. This binary file did not contain any personal data or any other data that, when decrypted, could link the "ballot" to the voter's identity. The file name contained only the date and time of the file. The "ballot" could be opened in any text editor, but it looked like lines of random characters.

Thus, the filled out ballot and data encryption were completely anonymous; no personal or other identifying information was stored in the encrypted file. If one wanted to be sure of anonymity, he or she could transfer the encrypted file to another computer and submit it from there.

C. Casting the ballot

Once the encrypted file was generated, the user was asked to choose the "Cast the ballot" function and then they were forwarded to the www.ipasas.lt website for authentication. Here his or her identity was determined using an online banking system or a digital signature. After the authentication was complete, the user was asked to upload his or her encrypted vote. As the "ballot" file was encrypted and the private key was not accessible, no one, even the administrators, were able to disclose the persons' "vote". The user could upload as many ballots as he or she wanted, but only the last vote counted. The previous votes were destroyed (overwritten).

Some of the data, such as the voter's age, gender, and IP-based location, was collected separately for statistic purposes.

The "last vote counts" principle was achieved in a very simple way using some basic principles of computer operating systems: two files with the same name cannot exist in the same folder. When the person identified himself or herself to the system, a unique number (a long integer) was generated based on the voter's personal code using a Hash function; thus, a unique number was created for each voter but the voter could not be identified backwards. This unique number was used as a file name to the encrypted ballot. So, after the voter authenticated himself or herself and uploaded the encrypted ballot file, the ballot file got a unique name generated by "hashing" the voter's personal code. Every other vote cast by the same voter got the same file name;

thus, it automatically overwrote the previous vote. This means that only the last vote is stored in the database, with no history (unless the database is somehow duplicated or backed up before the vote update). This allowed the existence of the "cancellation vote", a special instruction that could be sent to the server to delete the vote that was previously cast.

This explanation of the "last vote counts" principle was the easiest way to convince people that the ballots were actually not linked to the voter's identity, and there really was no way to disclose the secrecy of the vote in this phase.

A Youtube video [5] was made to demonstrate how the simulator worked.

V. The process

The simulation voting was launched on the 18th of September, 2012 at 12:00 after an announcement on www.delfi.lt, the largest Lithuanian news portal. An immediate reaction followed the launch. The promotional article was read more than 40 000 times, and readers left more than 1000 comments in just the first few hours.

More than 600 people tried the simulator on the first day.

The voting lasted for 17 days – until the 5th of October, 2012. A total of 3788 electronic "ballots" were uploaded (including "re-votes"). More than 30 000 users downloaded the voting application but never uploaded the ballot.

One hundred and two participants "re-voted" at least once. A total of 3566 valid ballots were counted.

One hundred and fifty-eight users downloaded the source code.

Every voter was offered a Certificate of Participation. (This was a generated PDF file with the user's name and surname, saying that he or she had participated in the first educational online voting simulation game.) The mayor of Vilnius and several ministers and members of Parliament were among those who proudly published their certificates on their Facebook timelines.

VI. Anonymisation, decryption, and tabulation of the results

After the "voting" period was over, the collection of votes was stopped and the anonymisation process started. The server with all of the "votes" was disconnected from the Internet first.

The process worked by simply randomizing the filenames of the ballot files. As we did not store a history of the votes, we had only the last "valid" votes; thus, randomization of the filenames was sufficient to ensure voter anonymity and that only one vote per voter was counted.

The Private Key was put back together and the decryption algorithm was then launched. The votes were decrypted and the results were then tabulated. The Private Key was then destroyed so any previously made (or backed-up) copies of the votes could not be decrypted.

VII. The results overview

As this simulation was widely supported by liberal-wing politicians and youth organizations, liberal (28,86%) and conservative (26,00%) parties "won the online elections". Of course, this did not correspond to the results of the actual elections of the Parliament that took place the week after the simulator ended.

Voter distribution was as follows:

- 1130 females (30 percent) and 2638 males (70 percent),
- 679 voters ages 18-24,
- 1603 voters ages 25-34,
- 861 voters ages 35-44,
- 408 voters ages 45-54,
- and 215 voters ages 55 and above.

Although the simulator covered most aspects of online voting protocol, some important aspects were missing and should be resolved before introduction in binding elections.

Firstly, anyone with a Lithuanian electronic ID or means of internet banking authentication could participate in the ivote.lt project, regardless of their citizenship or age. Only the ones included in the electronic voters' list could vote in real online voting.

Secondly, the ballots of the iVote.lt were all the same, and the person that downloaded this was completely unknown to the system. In real voting the voter would first identify himself or herself electronically, so the ballot issuing server could determine if he or she were eligible to vote and voting constituency, and then give him or her the respective ballot.

Thirdly, it was possible to authenticate to iVote.lt not only by digital signature, but also by means of internet banking. In real online voting internet banking is not a valid method of authentication. The voter would sign in using a digital signature or other means of electronic ID, depending on the legal framework.

Fourthly, ivote.lt did not offer an option for the voter to check if his or her vote was counted, which is becoming a standard in actual working online voting systems.

All other technological and organizational methods, including "The last vote counts", "Vote cancellation", and user interface meets the requirements for online voting systems, so it is only a matter of time and political will when this voting method will be implemented in our country.

VIII. Publicity and media coverage

As noted before, the ivote.lt was not only a piece of software, but also a publicity project. More than 20 popular articles were published on the major Lithuanian news portal delfi.lt, where different people (politicians, bankers, artists, scientists, and others) expressed their support for the

introduction of online voting. There were also articles on cyber-security, digital signatures, and digital identity.

Three big rounds of discussions were held in the headquarters of the Central Electoral Commission. All three events were webcasted live on the Internet and video reviews were made after. The first round gathered representatives of the media, business, and politics. The second round brought together all the leaders of the main political parties, and the third round included IT experts, journalists, and representatives of the expatriates. These discussions revealed the growing demand of society to introduce online voting, especially among expatriates and young, active people living in Lithuania. The IT experts agreed that the current IT infrastructure is sufficient to ensure the required level of security, but some politicians still expressed a high level of mistrust and kept declaring that "our society is not ready yet".

IX. Conclusions

The project was created to promote the idea of online voting and to explain to the general public how online voting might work. The users were able to test the possibilities and advantages of online voting by themselves.

The following conclusions were made:

1. More than 3500 people participated. That was twice as many as the authors initially expected.
2. The main objective of the project was achieved completely; i.e., a fully operational online voting module was presented to the public. It scoped every aspect of online voting procedure – starting with user authentication and vote encryption, and ending with depersonalization and tabulation of the results.
3. The project proved that anonymity of the vote can be guaranteed during all stages of online voting. This was clearly explained to the public.
4. Despite the fact that results of ivote.lt do not correspond with the actual results of the Parliamentary elections of 2012, wide distribution of votes among parties show that online voting is supported by citizens of various political views.
5. The geographical distribution of ivote.lt participants showed there is a possible increase in turnout of voters living abroad.
6. The gender and age statistics showed that online voting is supported by various ages among both genders.
7. The project drew a lot of attention from various fields of society and government; politicians, businessmen, journalists, and other public figures joined the online voting–related discussions.
8. Despite a number of attempts, we do not have any information that the system was ever hacked or influenced from the outside in any way.

X. Further Steps

The online voting simulator drew enough public attention to the idea of online voting. Despite obvious Estonian success, the introduction of online voting in Norway, and online voting for expatriates in France, there is still a lot of resistance and doubt among politicians regarding the introduction of online voting in Lithuania.

However, there have been small steps made in the right direction. For the first time ever, during the presidential elections of 2014 the candidates were able to gather signatures of their supporters online. The winner - current President Dalia Grybauskaitė - collected the required minimum of 20 000 signatures just online. A total of more than 60 000 signatures were collected online. This shows growing public confidence in e-democracy.

The amendment to the Law on Municipal Governance was submitted to the Parliament, which will allow anonymous public surveys (i.e., local referendums) by means of electronic communication. This will allow the creation of a fully-functional online pilot system that technically will meet all the requirements for national elections, and could be tested and evaluated without putting national-level elections at risk.

In the spring of 2014 the Minister of Justice, together with the Minister of Transport and Communications, announced that online voting will be introduced in Lithuania some time soon.

References

[1] First Lithuanian concept for internet voting. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=287235&p_query=&p_tr2=

[2] Electronic Voting: Algorithmic and Implementation Issues, Robert Kofler, Robert Krimmer, Alexander Prosser, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03).

[3] http://neu.e-voting.cc/wp-content/uploads/Proceedings%202006/1.1.madise_martens_e-voting_in_estonia.pdf

[4] Recommendation Rec(2004)11, adopted by the Committee of Ministers of the Council of Europe on 30 September 2004, was prepared by the Multidisciplinary Ad hoc Group of Specialists on legal, operational and technical standards for e-voting (IP1-S-EE).

[5] A link to a Youtube video, explaining how the simulator worked: https://www.youtube.com/watch?v=8akH1g0Iug4

[6] http://www.coe.int/t/dgap/democracy/Source/EVoting/EVotingReview06/JONAS%20UDRIS-Strasbourg2006.ppt