Challenges for Large-Scale Internet Voting Implementations

Kyle Dhillon
Princeton University Department of Computer Science
Independent Work Final Report, Spring 2015
Advisor: Professor Andrew Appel

Abstract

Several governments around the world have been experimenting with Internet voting as a means to make elections easier and more efficient. This paper explains how modern, large-scale implementations of Internet voting systems work and examines exactly why they are so difficult to secure, using two recent implementations of Internet voting systems as case studies. I then propose techniques for solving the problem of widespread public trust in Internet voting, and finally examine the potential for Internet voting systems that utilize fully end-to-end verifiable schemes.

1. Introduction

1.1. Background

Governments and citizens alike are constantly searching for ways to make voting more efficient and accessible to more people. Recently, various governments have been experimenting with Internet voting as a means to achieve these goals. In fact, multiple European countries have held binding national elections over the Internet several times in the last decade [1–3].

The security of such Internet voting systems is extremely important. In any election, there is the danger of fraud and coercion, and numerous cybersecurity experts have pointed out that

Internet elections are particularly susceptible to these threats, more so than traditional voting systems [4–6]. In this paper, I explain how modern implementations of Internet voting systems work and examine exactly why they are so difficult to secure, using two large-scale implementations in Europe as case studies. I then propose techniques for solving the problem of widespread public trust in Internet voting, and finally examine other options for Internet voting systems that use end-to-end verifiable schemes.

1.2. What is Internet Voting?

In this paper, I use the term “Internet voting” to refer to election systems in which registered voters have the option to cast valid ballots from their personal devices (which might include computers, laptops, tablets and smartphones). These ballots are transferred over the Internet to election officials and counted normally.

Internet voting is contrasted to “traditional voting,” in which voters must physically be present a polling place that is operated and monitored by election officials in order to cast their ballot. In traditional voting systems, voters may cast their ballot using a paper mechanism or by using electronic voting machines, which are generally not connected to the Internet.

When using the term “modern Internet voting systems,” I am referring to the large-scale Internet voting systems that have been implemented between 2005 and 2015, particularly the Estonian national e-voting system and the Norwegian pilot project voting system.

1.3. Supplementary Video: “Should We Trust Internet Voting?”

This research is supplemented by a related project: a video explaining to the general public why Internet voting is insecure. This video, which is four minutes long and titled “Should We Trust Internet Voting?” is meant as a high-level introduction to modern Internet voting schemes and the threats they face. A detailed look at the construction of this video can be found in section 5.

This video is currently available online at www.youtube.com/watch?v=hg34L_iMg6s.

2. Components of Modern Internet Voting Implementations

This section details the components of a typical Internet voting implementation. Because these systems must be implemented on a large scale and with usability in mind, they sacrifice several verification properties in exchange for ease of installation and use by voters.

Components of a typical modern voting implementation include:

- A master public/private key pair used to encrypt/decrypt all ballots
- An individual public/private key pair for each registered voter, used to digitally sign ballots
- Software on the voter’s device that encrypts and signs a ballot and transfers it to the vote forwarding server over the Internet
- A vote forwarding server, accessible over the Internet, which receives encrypted ballots, determines whether they belong to registered voters, and forwards them to the vote collection server
- A vote collection server that stores encrypted votes until vote collection is complete

- An offline protocol for decrypting and counting ballots after all votes are collected
- A second-channel individual verification method enabling voters to verify that their encrypted ballots were received by the central server

Not all modern implementations of Internet voting contain all of these components. Rather, this list is meant to represent components that the most secure modern implementations typically contain, specifically the Norwegian (2013) and Estonian (2015) voting systems [7,8].

2.1. Master Encryption/Decryption Key Pair

Most modern cryptographic voting implementations rely on public-key cryptography for ballot encryption. Before an election, election officials generate a master public-private key pair in a secure environment, for example, by using a Hardware Security Module (HSM) [7].

The master private key, which is used to decrypt votes, is divided among a number of election officials using a cryptographic technique known as *threshold encryption [9].* In threshold encryption, a certain minimum number of election officials must present their unique keys in order for the master private key to become available [7]. This technique minimizes the risk of leaking the master private key if a single key becomes public, and reduces trust requirements for each individual election official.

The master public key is embedded in the software used to encrypt voters ballots. It is important that both public and private keys are kept secret from the public, because if the public key were to become known, attackers could encrypt and submit illegitimate ballots [6].

2.2. Voter ID Key Pairs

Asymmetric cryptography is also used for ballot signing and voter identification. Modern cryptographic voting systems may issue a voter identification card to all registered voters, containing a unique private key for each voter. The list of all voters' public keys is stored at the election office and is only accessible to election officials [7].

Through the voting software, voters digitally sign their encrypted ballot with this unique private key. This act of digitally signing an encrypted ballot is analogous to vote-by-mail systems that require voters to place their marked ballots inside two envelopes: one unmarked inner envelope (represented by the encrypted ballot) contained inside an outer envelope containing voter identification information (represented by the digital signature) [7]. Digital signatures guarantee that each voter has control over the votes cast in their name, so long as their private key is kept secret.

2.3. Ballot Encryption and Transmission Software

A fundamental component of any Internet voting system is the software through which users cast their ballot. It typically features a user-interface by which voters first verify their identity using their ID cards or using login information, and then select their candidates of choice and confirm submission of their ballot. At this point, the software encrypts the ballot using the master public key which is embedded in the software. Finally, the software digitally signs the encrypted ballot using the voter's supplied private key, and sends it to the vote forwarding server [7].

This software may run in a voter's browser or as a standalone downloadable application [6,7]. This software is not required to verify that users are registered voters before sending signed votes to the vote forwarding server [7].

2.4. Vote Forwarding Server

The vote forwarding server (VFS) receives incoming encrypted ballots sent by voting software. By accessing a master list of all registered voters' public keys, it verifies ballots belonging to registered voters and discards unregistered ballots. It then forwards registered voters' ballots onto the vote collection server, which is not directly connected to the Internet. The VFS is the only component of the central election system that is accessible over the Internet [7].

2.5. Vote Collection Server

The vote collection server (VCS) receives ballots from the vote forwarding server. The VCS simply stores a database of all received encrypted ballots until the election is over [7]. In older Internet voting systems, the VCS and VCF were not separated, and rather were a single multi-purpose server [6]. Modern voting implementations tend to separate these servers, so the database of collected votes is not directly accessible over the Internet.

2.6. Offline Vote Counting Protocol

When the election is over and vote collection has terminated, voting officials typically have an offline process by which they can tally received votes. This first involves transferring the database of encrypted votes via removable storage media (USB thumb drive or CD-ROM), to a secure, offline, counting machine [6,7]. Election officials then access the master private key by pooling their individual keys using the threshold encryption technique described in section 2.1. The master public key is used to decrypt all ballots, which can then be counted by the counting machine.

2.7. Individual Ballot Verification Method

A relatively recent addition to these voting systems is the concept of individual ballot verification. Because the security of voters' own devices is difficult to guarantee, another communication channel (such as SMS or a smartphone application) can be used to verify that a ballot was properly received by the vote collection server. This is usually accomplished through a confirmation message indicating that a ballot was received from the voter, along with coded indication of which candidates were selected [10,11]. As discussed in section 3, while this additional verification option does partially solve the serious problem of insecure user-end devices, it violates the fundamental principle of ballot secrecy [10].

3. Overview of Modern Internet Voting Implementations

This section describes two specific implementations of Internet voting which follow the above protocol. There are, of course, many other governments which have attempted Internet voting or that will attempt it in the coming years. However, these two systems were selected primarily because:

1) they have both been implemented for national binding elections, and
2) they have both undergone rigorous security analysis.

Because each system follows a similar protocol to the one described in the previous section of this paper, I describe each implementation by its differences from that standard protocol.

3.1. Estonian e-Voting System (2005-2015)

Estonia is currently the only country in the world that allows Internet voting in their national parliamentary elections, and has employed such a system in seven different national elections since 2005. In the 2015 European Union Parliamentary election, roughly 20% of Estonian ballots (176,491 voters) were cast online [2].

The modern (2013-2015) Estonian Internet voting system is identical to the one described in section (2), and uses a smartphone app as a means to verify that a user's vote was properly cast [7,12]. Estonia also allows repeat voting as a means to combat coercion and bribery.

In 2014, researchers at the University of Michigan conducted a thorough security analysis of the Estonian Internet voting system [5]. Their research focused on discovering vulnerabilities in the client-side voting software and central servers, as well as procedural lapses in operational security that created opportunities for attackers to either disrupt the election, submit forged ballots, modify existing ballots, or change the way ballots were tallied. The details of these specific attacks are included in the following section.

3.2. Norwegian Internet Voting Pilot Project (2011, 2013)

Norway experimented with Internet voting in certain municipalities twice, first in 2011 and again in 2013. After the 2013 elections, Norwegian officials decided not to continue trials in the future, citing a lack of broad “political desire” as well as distrust in the security of the system as the principal reasons for the discontinuation [13].

The Norwegian system is nearly identical to the Estonian system described above, The Norwegian pilot project used a slightly different individual verification method to the Estonian one, based on the concept of “return codes.” Before the election, each voter receives a list of codes for each party running in the election. This list is unique for each voter. After a voter casts her ballot, she receives an SMS message containing the “return code” corresponding to her vote, and can therefore verify that her vote was properly cast [10].

Finally, Norwegian officials insisted that elections feature additional components of end-to-end verifiability based on zero-knowledge proofs. These would allow verifiers to mathematically prove that all votes were properly handled at various stages of the election. The notion of end-to-end verifiability is discussed in detail in section 6 [10,14].

4. Security Challenges of Internet Voting

4.1. Fundamental Requirements of Voting

Several fundamental requirements of any voting system, online or offline, are as follows:

- All votes must come from registered voters, who can cast a maximum of one ballot.
- The final vote count must accurately reflect all cast ballots.
- A voter must not be able to prove how she voted to a third party. In other words, the ballot-casting process must be receipt-free [15].

This requirement for receipt-freeness, which can be considered part of the principle of “ballot secrecy,” exists so that voters are protected against coercion and vote-buying.

In modern Internet voting systems with individual ballot verification methods as described in section 2.8, voters can receive confirmation that their vote was cast as intended. However, this confirmation message allows voters to easily prove to a third party how they voted, clearly violating the principle of ballot secrecy. Internet voting systems usually address this threat by allowing revoting, both online and in person at polling places. This means that if a voter was bribed or coerced to vote one way, they have the ability to recast their ballot as many times as they like. If a voter places an offline vote at a polling place, their online ballots may be nullified [7,10].

Although revoting may create a solution to this problem in some situations, it does not solve the fundamental problem that ballot secrecy has been violated and that vote-buying is now possible. Consider the following example: in the 2015 Estonian parliamentary elections, roughly 36% of registered voters, or 321,883 people, did not cast a ballot [2]. Suppose the majority of these people chose not to vote because they simply do not care enough about the election to waste their time voting. This group of non-voters would be highly susceptible to coercion and vote-buying, as they would be unlikely to exercise their right to place a second vote, considering they did not vote in the first place. Essentially, the "revote safety net" does not create a permanent solution to the problem of sacrificed ballot secrecy.

4.2. Challenges of Remote Voting

Remote voting, that is, voting not taking place at a polling station (including Internet voting and voting-by-mail), presents two additional challenges for a secure election.

First, remote voting makes identification of registered voters challenging. Internet voting systems solve this problem by using unique voter ID information and digital signatures, as described in section 2.2. However, if a voter's ID information is stolen, an adversary has the ability to place a legitimate vote in that voter's name. Some voting systems address this threat by giving voters a unique PIN code that must be provided before a ballot can be submitted [5].

Second, remote voting makes guaranteeing a secret ballot virtually impossible. As described in section 3.1, the secret ballot principle is fundamental to ensuring that voters will not be subject to bribery or coercion. Again, voting systems address this by allowing revotes, which are described more thoroughly in the previous section.

While these two fact -- that anyone can steal another's identification information and place a vote in their name, and that ballot secrecy is impossible to guarantee -- should be troubling, they are true of all postal voting systems which are commonly employed in large democracies [10]. So while these challenges should be mitigated in any remote voting implementation, they cannot be seen as problems unique to Internet voting.

4.3. Client-Side Vulnerabilities

Perhaps the biggest security challenge to Internet voting implementations are the insecurity of user devices. If a user's device is compromised, it could record a voter's private key and PIN and submit unauthorized votes in the client's name [5].

In their analysis of the 2013 Estonian national election, researchers implemented a number of client-side attacks that exploited these vulnerabilities. These attacks included a malware program that could silently replace a user's vote with a different one, while still tricking the smartphone verification software into believing a legitimate vote was cast [5]. Another attack directly compromises the smartphone verification app, rendering the verification software useless if both a user's computer and device are compromised simultaneously [5]. So while individual vote verification is intended as a safeguard against this kind of attack, a clever attacker can either manipulate the verification channel or devise an attack that bypasses the verification channel altogether, perhaps by submitting a new ballot at a later time [5].

4.4. Server-Side Vulnerabilities

The public-facing vote forwarding server (VFS), the vote collection server (VCS), and the vote counting machine are the most critical components of an Internet voting system. As such, they present the most attractive targets for adversaries, and must be secure against a wide variety of attacks. This is made more difficult by the fact that the VFS must be connected to the Internet and thus exposed to attackers from all over the world [7].

In their analysis of the 2014 Estonian election, researchers discovered multiple vulnerabilities in the Internet-facing vote forwarding server. For example, they discovered that the vote forwarding server is subject to a simple denial-of-service attack that could have prevented new votes from being recorded after roughly 75 minutes. These researchers also discovered a shell-injection vulnerability that could have allowed any election worker to execute shell commands with root permission on the vote collection server [5].

Although the vote collection and counting servers are not directly connected to the Internet, they are still vulnerable to attack. These same researchers implemented several attacks on the offline vote counting server of the Estonian election that could have silently changed

100% of votes during the tallying process. Before these servers are installed, for example, attackers could install malware on installation DVDs or on device firmware that could steal votes once vote counting begins. The researchers also noted additional attacks to this offline server, including during software updates and by exploiting zero-day vulnerabilities in third-party software [5].

4.4. Software Bugs

An unfortunate reality of large-scale voting implementations is the existence of bugs in software, either on the client-side or server-side. More formally, these bugs are mistakes in the implementations of these systems that result in unpredictable differences between the proposed theoretical system and the actual implementation. As an example, bugs in client-side software might expose voters' ballots to the public and violate the principle of ballot secrecy. In the 2013 Norwegian national elections, a bug was discovered in the encryption code that resulted in 29,000 virtually non-encrypted ballots being transferred to the central servers [14].

To minimize the presence of bugs, Internet voting systems typically publish their source code online, both so auditors can identify bugs themselves and for the sake of transparency. Unfortunately, this also makes vulnerabilities caused by minor bugs easy for attackers to find. In a 2010 Washington D.C. Internet voting pilot project, for example, researchers discovered a minor bug in the open-source client-side encryption software that ultimately gave them full control over the central vote collection server [6].

It is virtually impossible to guarantee the absence of bugs in any large software project. As a result, any Internet voting implementation suffers from the uncertainty of whether or not the implemented system exactly matches the desired one.

4.5. Undetectability of Attacks

Perhaps the most frightening aspect of these threats to an election is that they may be impossible to detect. The malware that could have forged votes in the 2013 Estonian election, for example, operated silently without alerting the voter or the central election servers, and could have changed hundreds of thousands of votes while still undetected [5]. In the 2010 attack on the Washington D.C. system, researchers had full access to the central server for several days before officials discovered their presence [6]. While steps can be taken to maximize the chances for detecting an intrusion, the nature of well-executed cyberattacks is that they tend to be completely undetectable.

4.6. Summary

The attacks mentioned above are unfortunately not an exhaustive list. Rather, they illustrate that implementing large-scale Internet elections is virtually impossible to do without creating numerous opportunities for voter-side and server-side attacks. The Estonian and Norwegian implementations in particular are two of the most advanced and thoroughly audited Internet voting systems ever implemented [3]. In the Estonian case, a small teams of researchers was able to discover a variety of attacks which could have, at the very least, disrupted the voting process and created a nightmare for election officials, or in the worst case completely fabricated election results. Any realistic threat scenario for a national Internet election should consider adversaries with far more computational and financial power than these teams. The sheer number of potential vulnerabilities, as well as the impossibility to predict additional vulnerabilities and the inability to detect attacks, are ample reasons to thoroughly distrust any modern Internet voting system.

5. Addressing Misplaced Trust in Internet Voting

Despite the insecurity of modern Internet voting systems, there exists widespread trust in these systems from the voting public as well as from public officials [1,2]. This trust has lead a number of governments, such as those listed above, to rush to develop Internet voting systems that may be seriously insecure. And although cryptologists and network security experts have been expressing serious concerns about Internet Voting for many years, these concerns tend to be buried near the end of technical security-analysis papers [4,6].

There have been efforts to educate the general public on the dangers of Internet voting. The most notable of these efforts is the website *estoniaevoting.org*, created by the same team that observed the security vulnerabilities of the Estonian voting system [16]. This website focuses specifically on the Estonian system and describes its vulnerabilities in terms that non-experts can understand [17].

However, there still exists a need for non-specific explanations of the risks of Internet voting, enumerated in simple terms. In an attempt to address this, I created a short video, titled “Should We Trust Internet Voting?” that explains the topics covered in this report in terms that should be understandable by the average, Internet-savvy voter.

The case I put forward in this video differs slightly from traditional arguments against Internet voting, because the concerns of the average voter are different from the concerns of a cybersecurity expert. The most important components of this argument are outlined in this section.

5.1. Rejecting Political Motivations

When hearing a case against Internet voting, a skeptical voter may suspect that the "expert" has political motivations. For example, a voter might wonder: is a political party paying this expert to dissuade people from trusting Internet voting, because it would hurt this party in the next election?

The aforementioned website *estoniaevoting.org* addresses this concern by emphasizing that the research team is "independent" and has "not accepted any financial support from within Estonia" [18]. In my video, I attempt to neutralize this concern by explaining my own frustration with traditional voting systems, and my own desire to see Internet voting realized. I frame the video as an explanation of careful research done into this problem from a variety of politically-neutral sources. Additionally, I spend time explaining end-to-end schemes that might work in the future. This implies that my concerns with Internet voting are simply with the current state of security, not with the concept itself.

Unfortunately, it is difficult to completely prove that one has no hidden political motivations. Despite the attempts of the University of Michigan research team to distance themselves from political motivations, the Prime Minister and President of Estonia have both insinuated that this team was "bought off by a rival political party seeking to disparage the system" [5]. Nonetheless, mitigating these concerns to the best of one's ability is critical to add credibility to any argument against Internet voting.

5.2. Use Voters' Fear

Though it sounds manipulative, capitalizing on a voter's natural fear of a stolen election is important to convince them to distrust Internet voting systems. After an Internet election takes place, there will likely be a similar fear among broad swathes of the general public, especially among those voters for the losing party. Future voters may often be too distracted by the promised convenience of Internet voting to consider the worst case outcomes and realities of a lost election.

I play off this fear in two ways in this video. I begin by emphasizing that the stakes in these elections are extremely high. I want this audience to understand the full consequences of a failed election before I discuss specific threats in more detail later. Second, I emphasize the fact that cyberattacks on voting systems are potentially undetectable, and that even an election that appears to run smoothly may be undergoing careful attacks from adversaries. This is, in my opinion, the most frightening argument to be made against the use of Internet voting systems.

Something I do not discuss in the video, but which is important to consider, is the aftermath of a close Internet election. If the election appears to have run properly, how would a losing party react? They would likely claim that there was fraud in the voting process, and it would be near impossible for the election officials disprove these claims. If officials detected a successful attack on a large scale, how might they operate a recount? These procedural ambiguities are extremely important to consider, but were not included in the video as a tradeoff for video length.

5.4. Level of Technicality

An additional consideration when making this case is the level of detail and vocabulary that should be used. Most Internet users are familiar only with the most basic concepts in computer security. Thanks to film, they recognize what a hacker is. From personal experience, they most likely know that personal computers are susceptible to viruses. Thanks to the 2013 NSA leaks, they're likely aware that government agencies have the resources to see and collect information about citizens' activity over the Internet.

At the same time, the average Internet user would initially be confused by the concept of public-private key encryption, which is fundamental to Internet voting schemes. They probably do not know that most Internet traffic, including email, is highly insecure. As a result, an explanation of Internet voting must strike a balance between specificity and understandability. In my video, for example, I do not refer to the vote encryption process as "public-key encryption," which might seem contradictory to the average viewer, but rather simply as "encryption."

The technical terms I use without explanation include "cyberattack/attack," "encrypt/decrypt," and "server," under the assumption that the target audience is familiar with these concepts. More advanced concepts, like "cryptographic voting protocol" and "end-to-end verifiable schemes," I explain with simple hand-drawn diagrams.

5.5. Other Considerations

In addition to the specific elements mentioned above, there are other principles I found important in explaining the dangers of Internet voting to the general public. For instance, I assume that the viewer's attention spans are fairly short. When creating this video, I aimed for a duration of 3-5 minutes, and ended up with a final product of around 4 minutes. I also use hand-drawn diagrams to explain more complicated topics in a simple way.

6. End-to-End Verifiability

A useful property for developing any Internet voting scheme is "end-to-end verifiability" (E2E-verifiability). E2E-verifiability can apply to both traditional electronic machine voting systems as well as Internet voting systems, and is used as a way to solve the problem of needing to trust the election process that collects and tallies votes. However, this term is slightly ambiguous, as some elections (including the Estonian and Norwegian examples) may be partially "end-to-end verifiable" without providing all of the guarantees of full E2E-verifiability. For the purposes of this section, we use the definition of E2E-verifiability proposed by Josh Benaloh, who pioneered the term in relation to electronic voting [9,19]. The requirements of a fully E2E-verifiable system are that:

1) voters can individually check that their ballots are cast as they intend (*individual verifiability*), and
2) anyone can check that all of the cast ballots have been accurately tallied (*universal verifiability*) [20].

6.1. E2E-Verifiable Internet Voting Schemes

We have already observed two methods for providing individual verifiability: the Estonian smartphone verification app and the Norwegian SMS return code system. However, we have not yet discussed how we can guarantee universal verifiability. The typical method to guarantee universal verifiability is by using zero-knowledge proofs [9,14]. These proofs can convince a verifier that the voting process proceeded correctly with high probability, without giving the verifier any knowledge about the actual content of votes used in the election.

The ability to verify proper counting by using zero-knowledge proofs is available at several stages of the Norwegian Internet voting system [14]. In that election, verifiers could ensure, for example, that the encrypted votes that entered the counting process were decrypted and counted properly. However, while election officials argued that they had created "complete end-to-end verification," they did not include all of the necessary components that make for true E2E-verifiability [14].

An example of a fully E2E-verifiable Internet election system is Ben Adida's HELIOS, which has been called "a recognized standard in Internet voting verifiability" [14]. HELIOS provides all the guarantees of E2E-verifiability, including the ability to view non-interactive zero-knowledge proofs verifying that each ballot was properly cast, and that the complete election tally was computed properly [21].

6.2. E2E Schemes and the Future of Internet Voting

These fully E2E-verifiable systems create same violations of ballot secrecy as the individual verification systems of the Estonian and Norwegian systems. As a result, the creators of HELIOS warn against using HELIOS for “public-office elections” in which fraud and coercion is expected [22].

However, the additional guarantees provided by E2E schemes remove the need for voters to trust both their own devices or to trust the servers and officials managing the vote forwarding, vote collection and vote counting processes. This is extremely appealing for Internet voting systems, as we have seen that these central components are sources of major vulnerabilities. As a result, E2E schemes are currently being researched by a team of scientists with the Overseas Vote Foundation as a possible solution to secure Internet voting online [20].

7. Conclusion

In summary, modern implementations of Internet voting systems have been shown to be highly insecure. Despite this, there is still worldwide trust in Internet elections and movement towards the development of new systems. As a result, cybersecurity experts should focus on explaining the dangers of Internet voting in terms that everyday Internet users can understand in to reduce these risks until serious improvements in Internet election security can be guaranteed.

The addition of individual-verifiability through code return systems does remove some trust requirements from these systems, but sacrifices the property of ballot secrecy. This observation suggests a fundamental tradeoff in any Internet voting system between election security and ballot secrecy. There may be potential in fully end-to-end verifiable voting systems that use zero-knowledge proofs to show both that ballots have been received and that they have been properly tallied without revealing any information about those ballots to the verifiers. If these systems succeed, they may offer a solution that eliminates the need to trust most components in a typical Internet voting system while also protecting ballot secrecy. For now, the biggest challenge to Internet voting remains educating the voting public about its dangers, reducing the risk of major fraud in an insecure Internet election.

Works Cited

1. Norway Ministry of Local Government and Modernisation (n.d.) What do the voters do and think? English Summary.

2. Statistics - Internet Voting - Voting methods in Estonia - Estonian National Electoral Committee (n.d.). Available: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics. Accessed 27 April 2015.

3. U.S. Election Assistance Commission (2011) A Survey of Internet Voting. EAC.

4. Appel AW (2006) Ceci n’est pas une urne: On The Internet vote for the Assemblee des Francais de l'etranger.

5. Springall D, Finkenauer T, Durumeric Z, Kitcat J, Hursti H, et al. (2014) Security Analysis of the Estonian Internet Voting System. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM. pp. 703–715.

6. Wolchok S, Wustrow E, Isabel D, Alex Halderman J (2012) Attacking the Washington, D.C. Internet Voting System. Financial Cryptography and Data Security. Lecture Notes in Computer Science. Springer Berlin Heidelberg. pp. 114–128.

7. Estonian National Electoral Committee (2010) E-Voting System: General Overview.

8. Cortier V, Wiedling C (2012) A Formal Analysis of the Norwegian E-voting Protocol. Principles of Security and Trust. Lecture Notes in Computer Science. Springer Berlin Heidelberg. pp. 109–128.

9. Benaloh J (2006) Simple Verifiable Elections. Microsoft Research.

10. Barrat J, Chevallier M, Goldsmith B, Jandura D, Turner J, et al. (n.d.) Internet Voting and Individual Verifiability: The Norwegian Return Codes.

11. Estonian National Electoral Committee (2013) What is Verification of I-votes.

12. Estonian National Electoral Committee (n.d.) Internet Voting - Voting methods in Estonia. Vabariigi Valimiskomisjon. Available: http://www.vvk.ee/voting-methods-in-estonia/.

Accessed 23 April 2015.

13. Norweigian Ministry of Local Government and Modernisation (2014) Internet voting pilot to be discontinued. Government.no. Available: https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/. Accessed 23 April 2015.

14. Report ESM (2014) Internet Voting Pilot: Norway's 2013 Parliamentary Elections. The Carter Center.

15. Karlof C, Sastry N, Wagner D (2005) Cryptographic Voting Protocols: A Systems Perspective. 14th USENIX Security Symposium.

16. Independent Report on E-voting in Estonia | A security analysis of Estonia's Internet voting system by international e-voting experts (n.d.). Available: https://estoniaevoting.org/. Accessed 27 April 2015.

17. Independent Report on E-voting in Estonia | A security analysis of Estonia's Internet voting system by international e-voting experts (n.d.). Available: https://estoniaevoting.org/. Accessed 27 April 2015.

18. The Team | Independent Report on E-voting in Estonia (n.d.). Available: https://estoniaevoting.org/team/. Accessed 27 April 2015.

19. Smyth B, Frink S, Clarkson MR (2015) Computational Election Verifiability: Definitions and an Analysis of Helios and JCJ.

20. E2E VIV Project - End-to-End Verifiable Internet Voting: Feasibility and Assessment Study | Overseas Vote Foundation (n.d.). Available: https://www.overseasvotefoundation.org/E2E-Verifiable-Internet-Voting-Project/News. Accessed 27 April 2015.

21. Helios v4 - Helios (n.d.). Available: http://documentation.heliosvoting.org/verification-specs/helios-v4. Accessed 28 April 2015.

22. Helios Voting (n.d.). Available: https://vote.heliosvoting.org/faq. Accessed 30 April 2015.