Comparison of e-Voting Schemes: Estonian and Norwegian Solutions

Mohammad Jabed Morshed Chowdhury
Daffodil International University
Dhaka, Bangladesh

ABSTRACT

An increasing number of elections have been performed using Online Voting including Estonia, Canada, Norway and Switzerland. In October 2005, Estonia organized countrywide remote e-voting. Every Estonian citizen got the opportunity to cast their vote via Internet from all over the world. Approximately 2% of actual voters made use of this opportunity. Different countries are also working on to develop their own e-voting system. Inspired by the recent development, Norwegian government has also decided to develop e-voting system in the country. Norway's internet voting pilot project held in 2011 and countrywide e-voting will be held in 2017. Due to these experiences, the technical research topics have changed: While voting protocols have been well analyzed in the past, but little research has been done on the performed system. This paper will investigate the security and trustworthiness of the performed online voting. For this paper study and examine Estonian and Norwegian online voting system.

Keywords

e-voting, security, SMS attack.

1. INTRODUCTION

Electronic voting is already in use in many countries in the world. It is proved that it speeds up the counting of votes and improves turnout among disabled voters. Estonia is the first country which arranged countrywide e-voting and pioneer in e-voting system. It arranged e-voting in 2005, 2007 and 2009. The results of these elections are so far very positive. The system has been upgraded continuously. In 2011, Estonia introduced mobile authentication system.

Norway is one of the most developed countries in the world. The IT infrastructure of Norway is very good. They have introduced IT in almost in every spare of life. In the process to march towards an e-society, Norway is now planning to introduce e-voting. In 2011, an e-voting pilot project has covered some municipalities. They will have a nationwide e-voting in 2017.

Though Estonia is pioneer in this field but the e-voting system used here is not robust and secure. There are some major vulnerability in the system. Norwegian system has taken these vulnerabilities and loop holes into consideration to develop their system. In this paper, Estonian and Norwegian schemes are described in section 2 and 3.

To ensure a safety guard against malicious voter's computer, Norwegian protocol uses mobile phone as a channel of communication. Estoian voting system has also introduced mobile ID as an authentication mechanism for e-voting. But recently, there are also few vulnerabilities have been found in mobile phone system. In this context, different kinds of SMS attack are described in section 4. Section 5 has a comparative study of both the schemes and section 6 contains the concluding remarks.

2. ESTONIAN e-VOTING SYSTEM

Estonia is credited to be a pioneer in e-governance and e-democracy. The use of digital channels for different services is steadily widening, nearly half of house-holds have a computer at home and more than 4/5 of those are connected to the Internet. Estonia is among the first few countries in the world, where ID card with remote identification and binding digital signature functions is compulsory for personal authentication. Almost all Estonian inhabitants are already electronic ID cardholders. Therefore introducing e-voting was a logical step to take.

2.1 Background

e-voting could be seen as an essential convenience in an information society, like using Internet for sending tax declaration, car registration and online banking etc. e-voting has been actively discussed in Estonia on different levels since the beginning of this century. The IT infrastructure and peoples motivation has been a driving force to implement such a project. Participation in e-voting system is also growing fast since its first deployment. The voters who have voted electronically in 2005, 2007 and 2009 are respectively 0.9%, 3.4% and 9.5% of all the eligible voters [1].

2.2 Legal Issues

According to the Estonian Constitution, members of the Riigikogu as well as local government councils shall be elected in free elections based on the principle of proportionality. Elections shall be general, equal and direct, and voting shall be secret. There exists a legal basis for carrying out e-voting which is laid out in the following legal acts:

- Local Government Council Election Act
- Riigikogu Election Act
- European Parliament Election Act
- Referendum Act

2.3 Architecture

The main principle of e-voting is that it should be as similar as regular voting. It must be compliant with election legislation and principles and be at least as secure as regular voting [2]. Therefore e-voting must ensure the free will of the voter and voter's anonymity. The voting system must be secure, reliable and accountable. Since cohesion in the voting process is a major concern, the voting system should have mechanism to combat against any kind of coercion. Access to the voting system is also important, so the voting system should be easily accessible from anywhere and in almost in all popular platforms.

In Estonian scheme the following measures are taken in e-voting system to fulfill the above mentioned requirements.

1. For voter identification ID-cards or Mobile ID is used
2. e-Voter can vote any number of votes during the advance voting time. The final vote will be counted. Thus if voter is under any kind of pressure to vote, she/he can vote later and the last vote will be counted. It will ensure coercion free voting.
3. The priority of traditional voting. If the voter cast his/her vote in the polling station then all his/her e-vote will be cancelled.
4. All the servers in the voting system are secure and always under monitoring during the voting period.
5. Vote storage server is behind the firewall. Nobody can access the vote storage server from open Internet.
6. Vote counting server is offline and secure with shared private key.
7. All the communications in Internet use SSL encryption.
8. Encryption and digital signature use RSA encryption mechanism.

In general, the e-voting concept is similar to envelope method used during advance polls today to allow voting outside of polling place of voters residence. In e-voting a voter also creates an inner envelope (which is essentially an encrypted vote) and an outer envelope (which is essentially a digital signature). Then she/he sends this encrypted and signed vote to the voter forwarding server. Encryption of the vote provides confidentiality and digital signature ensures voter's authenticity.

In figure 1, the core architecture of Estonian e-voting system is shown. A detail description of the voting system can be found at [2]. In brief, the whole procedure is like this,

The voter goes to the voting website and authenticates himself to the website by his digital ID card. After authentication, he downloads the voting client application and installs it in his system. For e-voting, he runs the client application and authenticates himself to the system. The voting client application authenticates the voter to the system by collaboration with Vote Forward Server (VFS). After the authentication, the VFS gives him the candidate list of his constituency. Voter chooses the candidate from the list. Then the client application encrypts this vote by the public key of the Vote Counting Server(VCS) and signed it by the voter's personal digital signature. This encrypted and digitally signed vote is then forwarded to VFS.

VFS sends this vote to the Vote Storage Server (VSS). VSS communicates with the PKI system and verifies the identity of the person. It stores the vote and sends the confirmation to VFS. VFS sends the confirmation to the client. When the voting period is over, VSS sorts and cancels vote based on double vote and paper vote. VSS removes the digital signature of the vote after the advance voting time. Now no vote is linked with any kind of signature. By this way the anonymity of the voter is ensured. The voting personnel then takes all the encrypted votes and put them in the Vote Counting Server(VCS) in Offline.

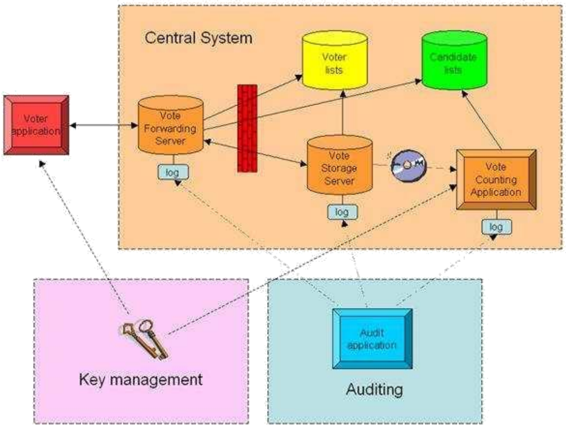

Fig. 1: Estonian e-voting Scheme [2]

In VCS, more than one person put their private key that combines the private key for the VCS and decrypts all the vote. VCS then counts all the votes and generates the result. The system always keeps logs of all the information. Later these logs are analyzed to examine security violations.

The following two functional requirements that e-voting system are often subjected to discussion but which are not accepted in the Estonian law for e-voting. The technical solution of e-voting does not directly support these two requirements. In fact both of them are realized on the basis of the principle of supremacy of conventional voting.

- The possibility to annul ones already given vote.
- Possibility to give an empty vote possibility to vote for no-one or to give an empty vote.

2.4 Mob-ID

From 2011, Estonia is going to introduce mobile e-voting. In fact, it is not a voting system from mobile rather it is an authentication system by mobile phone. The procedure is as follow:

1. In the client application, anyone can authenticate himself by e-ID or Mob-ID. The voter has to register his mobile phone from appropriate authority to have his mobile ID (Mob-ID).
2. If anyone wants to authenticate by Mob-ID, he has to enter his mobile number. He will get a code in this computer screen and will also get a SMS in his mobile phone.
3. He can validate the code by comparing both codes. If both code matches, then he has to give his pin number in the computer screen. After that he will see the candidate list.

4. He can select the candidate from the screen. Before submitting his vote he has to give his pin number again to sign the vote with his digital signature.
5. Then the encrypted and signed vote will be sent to VFS.

The architecture of the Mob-ID is shown in fig. 2. A detail description of Mob-ID can be found here [3].

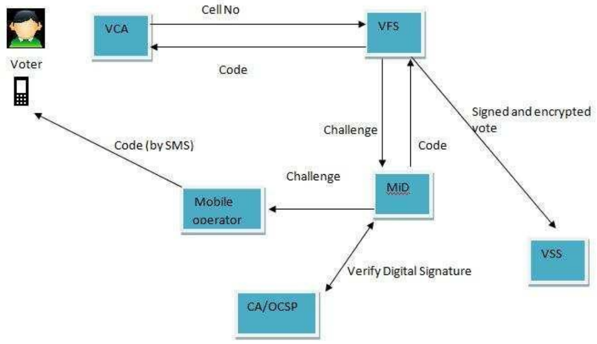

Fig. 2: System architecture of Mob-ID

A national agency will be responsible to maintain the system and ensures the security of this system. Since mobile phone is used as an authentication method, a strong trust between the government body and mobile phone operators is needed. Since the maximum mobile phone operators are privately owned, special attention should be given for any kind of security violation.

2.5 Security Analysis

Major security requirements for e-voting are authentication, voter's anonymity, freedom to chose and universal access. Security requirement of e-voting system can be grouped into five subgroups. The subgroups are central system architectural requirements, central system applications requirements, ensuring reliability, data format requirements and external data channels. Each sub component has associated risk involved. But the security requirement for different subgroups are quite different. The central system needs both technical and physical security while other subgroups need to be technically secure. There are few risks involved in e-voting system. The common source of vulnerabilities are,

- Failures and quality problems of voter application
- Man-in-the-middle attacks against web server and voters computer,
- Exposure of voter application or its input data
- Traditional web application/ web server management and security errors
- Failures and quality problems of Central Voting StorageSystem (VSS) soft-ware
- Functional failures of Voting Counting Server(VCS)
- Destruction/ inaccessibility of VCS secret key

The vulnerabilities in Estonian system: Risk should be identified in every level of e-voting process. It needs to identify the risk involved in the system component , e.g, VCA, VFA, VSS etc. Different components of the voting system have different kinds of security vulnerabilities and loop holes.

Voter's Computer(VC): Malicious voter's computer is the main source of security vulnerability in Estonian voting scheme. Usually the common people are not concern about security of their computers. It is quite common that voters computer is under malicious attack. The computer could be virus affected or affected by any kind of malware. A malicious computer can cast a vote without concern of the voter.

Voter Forwarding Server(VFS): The communication link between voter's computer and VFS is open Internet. There are different kinds of attack are possible in this communication link. Internet connection provider can stop the traffic or delay the traffic. Since VFS is in open Internet, DoS attack is also possible against VFS.

Voter Storage Server(VSS): As VSS stands behind the firewall, it is relatively secure than VFS. VSS stores all the votes, sorts them (only the last vote is casted) and cancels them(if voter votes in polling station). It also communicates with Public Key Infrastructure (PKI) for the public key of the voter. VSS database application faults enable irregular access to data and ignoring restrictions, therefore the fault-freeness of VSS applications is also a major security issue.

Voter Counting Server(VCS): VCS is the most important component in the system. The public key of VCC is open to all voters and used in encryption of the vote. VCA private key should under no conditions become public and must not under any circumstances be destroyed or become unusable. The source of vulnerability in VCS is from operating system, memory or any kind of virtualization.

Voter's Anonymity: VSS has encrypted and signed vote. VSS can identify the voter from this encrypted and signed vote but cannot decrypt the vote. Only VCS can decrypt the vote. If VFS and VCS both are corrupted then it can violate the voter's anonymity. Because VSS can unwrap the digital signature and mark the vote by time stamp or any other means then can send this to VCS. VCS can decrypt the vote and learn about the choice. Now if VSS and VCS collaborate together it can identify the voter and learn about his choice.

Mobile Related Attacks: There are few attacks possible against mobile phone system. SMS attacks, SMS injection and DoS attack on mobile phone are not rare anymore. An adversary can change the SMS code or block SMS to voter's mobile phone. A detail description of different SMS related attacks is given in chapter 4.

3. NORWEGIAN e-VOTING SYSTEM

The main feature of Norwegian e-voting scheme is its openness [5]. Norwegian government is trying to build trust on e-voting by making all the documents related to voting publicly available. They have released all the documents related to architecture and other technical matters. They have also decided to open the source code for the public to investigate the security holes.

The architecture of the Norwegian setting provides security measures against the two major issues, compromised computers and coercion in e-voting. It has introduced two independent channels(postal mail and SMS) to provide safeguard against compromised voter's computer.

The cryptographic protocol to be used in Norway is designed by Scytl, a Spanish company [5]. They have used a standard voting framework and have added two channel mechanism. In this protocol, anyone can vote for as many times as he/she likes in the advance poll time. Though homomorphic tallying is very popular for counting votes because of its simplicity. But in Norwegian setting, mix-net is used for the efficiency and security.

3.1 Background

For last few years it has been observed that people are practicing the advance vote which shows the change of the traditional voting practice. People are also more reluctant to use their voting rights. These two behavioral change of the voter, makes e-voting a good alternative to the traditional voting system. In this reality, in 2009 the Norwegian Ministry of Local Government and Regional Development (KRD) decided to start a procurement procedure for E-valg 2011, an e-voting pilot project for the municipal and regional elections of 2011 [5].

3.2 Legal Issues

Legal framework is always the most important aspect to introduce e-voting in any country. Constitution and Acts are the main guidelines for any election system. Norwegian constitution is very friendly for implementing e-voting. The legal framework is ready for e-voting in the country [6]. The main directives for e-voting in the constitution are as follows,

- It is illegal to mutilate voting results
- It is illegal to coerce a voter to vote or cast a vote against his or her will
- It is illegal to act negligently for the purpose of failing to count somebody’s casted vote
- It is illegal to sell an entitlement to vote
- It is illegal to buy someone’s vote

3.3 Architecture

Norwegian scheme also uses double envelope system to provide security and voter’s secrecy. The voting procedure [6] is as follows ,

1. Voter gets a post mail containing all candidates name and their verification code. It is different for each voter. The voter can compare this code later with the SMS code to verify that his vote is correctly casted or not.
2. The voting application authenticates the voter to the voting server with his national ID (eID).
3. The voting application receives a list of parties and candidates from the server via a secure channel; this list is not encrypted and the same for all voters in the same district.
4. The voting application displays the list of parties in a point-and-click inter-face, ordered randomly.
5. The voter makes his decision by clicking on the party name, and clicks on the Next button to continue. He has also the option to vote blank.
6. In the next step, the client application shows the candidate list for the party he selected, and allows him to give a personal vote to as many candidates as he wishes.
7. In the last step, a summary of the voter’s choice is presented. If the voter is happy with his choice, he can click on the Next button to encrypt and digitally sign the ballot, and send it to the server. The vote will be encrypted with the public key of the counting server and digitally signed by his own signature.
8. After casting the vote the voter will get the verification code in his mobile. He can check whether his vote is register for the candidate he voted or not by matching the code in the mail. If not he can revote for his candidate again.

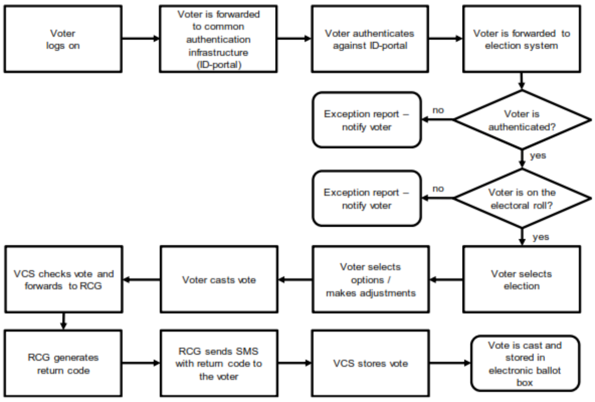

Fig. 3: Voting Process in Norwegian Setting

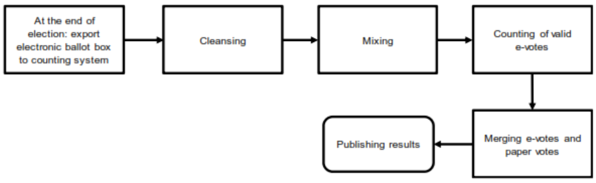

Fig. 4: Counting Process in Norwegian Setting

The main voting architecture is same as Estonian setting. The major differences are to use two channels to combat compromised voter’s computer and organized auditing system. These two channels are pre channel and post channel. Pre channel is normal postal mail and post channel is mobile phone.

In figure 3, voting scheme with 2 channels for voter is presented. Voters ballot (vote) is encrypted and signed (possibly by the attacker), and then sent to the vote collector. The vote collector computes, given an encrypted and signed vote, a ciphertext of the integrity check code Codev[cnd] and sends it to another server (called the messenger). The messenger decrypts the code, and then sends an SMS alert of the type You, [name], voted at [time], the check code is Codev[cnd] to the voter over post channel. The voter verifies the correctness: she complains when she got a wrong message over post channel (which say contains a wrong check code), or did not get it all when she voted (in particular when her computer tells her that the vote collector is unavailable), or gets a message when she did not vote. The detail of the procedure is described here [7].

The protocol needs a messenger, which can be behind a firewall, is unaware of the correspondence between the candidates and the corresponding check codes. A malicious messenger should not collaborate with a malicious vote collector. A detail cryptographic proof can be found at [7].

3.4 Security Analysis

Different kinds of attacks on e-voting system are described in [8]. There could be internal attack from insider like legitimate users, system developer and system operator. There could be attack from outside. Anyone can attack the system by hacking, Denial of Service (DoS) attack, malicious attack etc. There could be attack from individual, organization or from a terrorist group.

The vulnerabilities in Norwegian system: Though Norwegian system is better and more secure but it has also some security vulnerabilities. Introduction of two channel has solved the malicious voter's computer problem but it also brings some vulnerabilities. Some of the major vulnerabilities are described here,

Printing house: In pre and post channel setting, voter will get printed code for each candidate before the election. He can later verify the mobile message against this code for each candidate he has voted. Electoral body has to send each citizen this code. The volume of this printing will be very large. Someone can steal the code from the printing house. Adversary can attack the printing house IT infrastructure like Stuxnet attack in Iran [9].

Postal system: The code will be posted to each citizen. In general Norwegian postal system is secure and trusted. But some adversary can also learn the code by breaking the security of the postal system by stealing anyone's personal authentication document.

False claim: Voter gets the confirmation code in his mobile phone after casting his vote. If a voter claims that he has got wrong code intentionally, there is no instant mechanism to verify him wrong. In this way, if a group of people do this intentionally it will create mistrust among the citizen. It is not a technical attack but it will give a misconception among the common people.

SMS attack: SMS attack could be a good option for the adversary to attack Norwegian system. In Norwegian setting, voter gets the confirmation code in his mobile phone after casting his vote. Adversary can attack mobile phone infrastructure or individual mobile phone and send wrong code. An attack is possible that will block all incoming SMS to the user. There could be few other kinds of attack, e.g, DoS attack, SMS virus, SMS injection etc are also possible. SMS attack is a major source of attack possible on Norwegian voting scheme. A detail description of SMS related attacks is presented in chapter 4.

4. SMS ATTACK

SMS attack is described here in details as it is one of the major vulnerable part of the Norwegian setting. In Estonian setting there is also a procedure for mobile authentication. In this perspective, this paper tries to investigate all the SMS attacks possible on the mobile phone system.

- Security problems of SMS system:
- It is hard to prevent SMS attacks because user interaction is not required to send a massage (SMS).
- No possibility exists to firewall or filter SMS messages.
- Uncertainty of whether a message is delivered to the target in its original form.
- Mobile phone operators have the ability to filter and modify short messages during delivery.
- Some equipment that cannot handle certain messages.
- SMS is an unreliable service, meaning messages can be delayed or discarded for no deterministic reason
- Denial-of-Service attacks
- Vulnerability allows to disconnect a device from the mobile phone network
- SMS bugs (e.g, Curse of Silence bug which existed in most of Nokias Symbian S60-based smart phones)

4.1 SMS Injection

There are few ways to utilize the security holes in the mobile set specially in smart phone. SMS injection [10] is one of the most serious attack against mobile phone. SMS injection is based on adding a layer between the serial lines and the multiplexer (the lowest layer of the telephony stack). This new layer is called the injector. The purpose of the injector is to perform a man-in-the-middle attack on the communication between the modem and the telephony stack. The basic functionality of the injector is to read commands from the multiplexer and forward them to the modem and in return read back the results from the modem and forward them to the multiplexer. To inject an SMS message into the application layer, the injector generates a new cellular Messaging Teleservice (CMT) result and sends it to the multiplexer just as it would forward a real SMS message from the modem. It further handles the acknowledgment commands sent by the multiplexer.

Fuzzing Test Cases: SMS injection attack can explore the different security holes in the mobile system. The following are the different procedures to implement a SMS injection attack in a mobile system,

- Basic SMS Messages: It can be fuzzed various fields in a standard SMS message including elements such as the sender address, the user data (or message), and the various flags.
- Basic UDH Messages: It can be fuzzed various fields in the UDH header. This included the UDH information element and UDH data.
- Concatenated SMS Messages: Concatenation provides the means to compose SMS messages that exceed the 140 byte (160 7-bit character) limitation.
- Port Scanning: UDH Port Scanning for exploitation.

4.2 SMS Virus and Other SMS Attacks

The new smart phones are more vulnerable to SMS virus. There are many new SMS virus has been reported for Nokia, iPhone and android platform. The pernicious message exploits a bug in the Nokia phone software and, if received, will render some handsets completely unusable.

Dos Attack on Cell Phone: Mobile phones use the same small portion of radio frequency, called the "control channel," to both set up calls and send SMS messages, a flood of SMS messages could so overwhelm a cellular tower that it would effectively prevent any new telephone calls from going through. To be most successful, the attack would need to target telephones within a certain geographic region, but the researchers said that this can be done by using public databases and creative Google searches.

Attackers could build up databases of mobile numbers from specific regions and then flood those numbers with unwanted text messages. Attackers could use publicly available Web sites or messaging clients on zombie computers to send the text messages, which could eventually jam up the cellular towers that carriers use to send and receive SMS messages from mobile phones.

Trojan Sends Spam: Trojan hijacks PCs and uses them to send SMS-based spam to mobile phones. After a PC has been infected, the Trojan contacts a Web site for details on which spam campaign to run and then randomly generates a series of mobile numbers beginning. It uses the ”send e-mail” function of a number of mobile network Web sites to actually deliver the mail sent from the infected machines.

Black Hat: SMS Attacks: This report [11] says that all most all the GSM phones are vulnerable to anti-spoofing and they send data designed to get access and take control of the phone.

GSM Intercept Attack: The GSM protocol requires that any mobile handset that wants to join a network authenticate to the GSM network. But, the protocol doesn’t mandate that the network authenticate itself to the handset. By using this loop hole a fake base station can attach a cell phone to this base station. A device called an IMSI (International Mobile Subscriber Identity) catcher is designed as a fake GSM base station. It trick the target handset into sending its voice traffic and text message.

From the above discussion it is clear that different kinds of SMS attack are possible in the mobile phone system. As both these protocols depend on SMS based service,voter should be aware of this kind of attack. The system designer of the e-voting system should also consider this kind of attack against e-voting system.

5. COMPARISN

The basic architecture of both the voting system is almost same. Norwegian scheme uses two channel mechanisms to protect against malicious voter’s computer. This makes it more secure than Estonian system. The auditing system is also better in Norwegian system. Though Norwegian system is more secure and robust, it has also few security vulnerabilities. The comparison between two schemes can be shown in the following way,

5.1 Vote Verification:

In Estonian setting there is no way to know for whom the vote has been casted. But in Norwegian setting, voter knows for whom his vote has been casted. So, if he finds that he has got wrong candidate code then he can re-vote. In Estonian setting voter can only know that his/her vote has been stored in VSS.

5.2 Guard Against Vulnerable Voter Computer:

There is no mechanism to protect the voting system against vulnerable voter’s computer in Estonian setting. But in Norwegian setting two channel mechanisms is used to combat this vulnerability. Since the Norwegian system uses two different independent channels, it is very difficult to attack both the channels. If anyone of these channels is unaffected, the voter can easily identify the attack. Even if the computer is corrupt the voter can always identify it.

5.3 Vote Blank:

In Estonian system, a voter can submit a blank ballot in the conventional voting system. But in e-voting system, he cannot submit a blank ballot. On the other hand, in Norwegian system, the voter can submit a blank vote in e-voting system.

5.4 Using Mix-net for computing votes:

Homomorphic tallying is very popular because of its simplicity but in Norwegian setting, mix-net is used. In mix-net the computation is more efficient and secure.

5.5 Mobile authentication system:

There is no provision for mobile authentication in Norwegian system. But in Estonian setting voter can register for a mobile ID and later can authenticate himself with the system by his mobile ID.

5.6 Auditing System:

In Esonian setting the audit system is not organized and more of manual work. The system administrator usually goes through all the logs and checks for any security violation. On the other hand, in Norwegian setting the audit system is more automatic. The auditor verifies the content of the ballot box (signatures and proofs), that no ballots have been inserted or lost compared to the receipt generator list and computes on its own a list of encrypted ballots that should be counted. The auditor compares this list to the ciphertexts input to the mix net, then verifies the proofs offered by the mix net and the decryption service. The auditor also publishes hashes of every ballot, so that voters can verify that their ballots were included in the count.

6. CONCLUSION

This paper presents a comparison between Estonian and Norwegian e-voting sys-tem. This paper also investigates different SMS attacks. But this paper does not give any cryptographic comparison between these two schemes. Because there is no publicly available document related to cryptographic procedure of Estonian e-voting scheme. To prepare such a document can be a good research topic and future work. In general Norwegian setting is more secure and distributed. Still it has some vulnerabilities, which should be addressed and fixed before the deployment in 2017.

7. REFERENCES

[1] Internet voting in Estonia: www.vvk.ee/public/dok/Internet Voting in Estonia.pdf

[2] Working Committee: E-Voting System. www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf(2005)

[3] AS Sertifitseerimiskeskus: DigiDocService spetsifikatsioon. http://www.sk.ee/files/DigiDocService spec 2 123 est.pdf (01.03.2009)

[4] Arne Ansper, Ahto Buldas, Mart Oruaas, Jaan Priisalu, Anto Veldre, Jan Willem-son and Kaur Virunurm: E-voting conception security: analysis and measures. http://www.vvk.ee/public/dok/e-voting-security.pdf (15.12.2003).

[5] Kristian Gjosteen: Analysis of an internet voting protocol. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e valg/Nyheter/core.pdf (March 9, 2010)

[6] Working Committee: Electronic voting challenges and opportunities. Ministry of Local Government and Regional Development, Norway (2006)

[7] Arne Ansper, Sven Heiberg, Helger Lipmaa, Tom Andre Overland, and Filip van Laenen: Security and Trust for the Norwegian E-voting Pilot Project E-valg 2011. NordSec '09 Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age (2009)

[8] Working Committee: e-Vote 2011 Security Objectives. Ministry of Local Govern-ment and Regional Development, Norway (2009)

[9] Stuxnet attack: http://www.zdnet.co.uk/news/security-threats/2010/09/26/iran-confirms-stuxnet-attack-on-nuclear-site-40090272/ (last access time 7nd Decem-ber)

[10] Collin Mulliner and Charlie Miller: Injecting SMS Messages into Smart Phones for Security Analysis. WOOT'09 Proceedings of the 3rd USENIX conference on Offensive technologies, (2009)

[11] Black Hat: SMS Attacks: http://www.tipb.com/2009/07/30/black-hat-sms-attacks-iphones (last access time 2nd December).