UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

SECURITY IN DIGITAL SYSTEMS

THESIS

Topic: Electronic Voting. Analysis of the status &functionality and components of electronic voting. Development of methods on how creating trust relationship between E-voting system & voter/client.

MSc.Student: ZacharopoulosDimitrios

Assistant Professor: Lamprinoudakis Konstantinos

ATHENS 2015

Περιεχόμενα

Abstract of the e-voting 6

Introduction 6

Literature Review 8

1 Chapter Meanings 8

1.1 What is E-voting? 8

1.1.1 Paper Voting (Classical elections) 8

1.1.2 Description of the e-voting system 9

1.2 Definition E-vote 9

1.2.1 Definition of trusted system (E-voting) 11

1.3 Classification of e-voting 11

1.3.1 Polling station 11

1.3.2 Home with voter's computer 11

1.3.3 Voting with mobile devices 12

1.4 E-voting in controlled or uncontrolled environment 12

1.4.1 Voting Entities 12

1.5 Technology Problems in E-voting system and problems identification 14

1.6 Functionalities of E-voting Systems 15

1.6.1 E-voting without independent evidence of ballots casting 16

1.7 Description of EVS technologies 17

1.8 Practical Cases (Proposed systems) 19

1.8.1 UK pilot 20

1.8.2 Switzerland 21

2 Chapter Infrastructure of electronic voting system 23

2.1 Infrastructure of E-voting system 23

2.1.1 Pre voting stage 23

2.1.2 Registration process 24
2.1.4 Post stage 25
2.2 Cryptographic scheme's 26
2.2.1 Categories: 27
2.3 Categories of cryptography at e-vote 28
2.3.1 Mix Networks 29
2.4 Threats (General idea) 31
2.4.1 Denial of service Attacks (D.O.S) 31
2.4.2 TCP death 31
2.4.3 Packet malformation 32
2.4.4 Virus 32
2.4.5 Trojan Horses 33
2.5 Physical Attacks in the E-voting 33
3 Methodology 35
3.1 Purpose of thesis 35
3.2 Methodology of research 35
3. 3 Design 35
3. 4 Results 36
4 Chapter Confidence 37
4.1 Trust 37
4.2 Layers of trust 38
4.2.1 Issues Influencing trust in e-voting system 40
4.2.2 Explanation of confidence (1) 42
4.2.3 Trust view (2) 43
4.2.4 Trust in e-voting process 43
4.3 Social Content 44
4.3.1 Political Aspect 45
4.3.3 Time 46

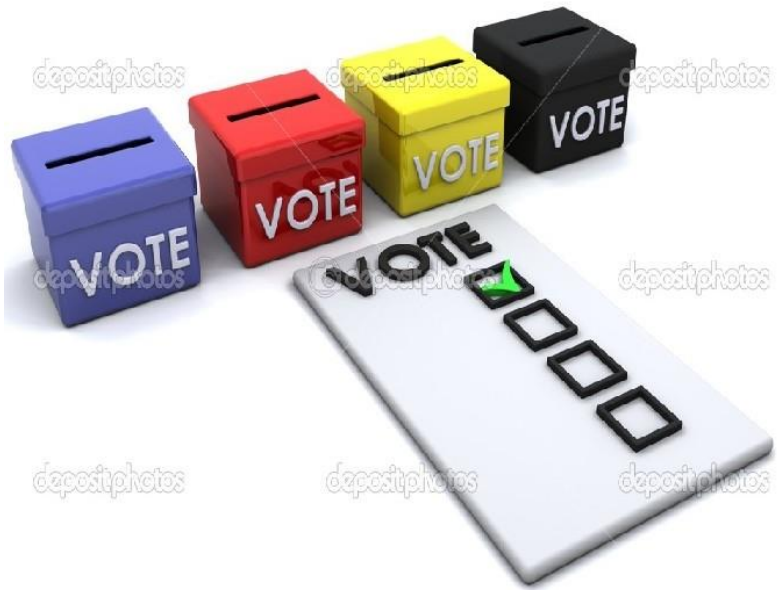
4.4 Categories of trust 47
4.4.1 Access Trust (Resource) 47
4.4.2 Provision Service by the trustee 47
4.5 Certifications 48
4.5.1 Delegation trust 49
4.5.2 Infrastructure Trust 49
4.6 Trust Management 50
4.6.1 Trust Management solutions 51
4.7 Preview of trust issues about previous e-votingenvs 52
4.7.1 Trust in e-voting (political elections) 52
4.7.2 Trust at stages of e-vote 53
4.7.3 Trust flow during casting 53
4.8 CIA 54
Confidentiality Threats 54
Hardware and Software 55
Integrity threats: 55
Authenticity 55
5 Chapter functioning & non functioning 57
5.1 Security & Technical Requirements 57
5.1.1 Requirements for e-voting system in depth 57
5.2 Tallying stage requirements 59
5.3 Accuracy 61
5.4 Voter Authentication 62
5.4.1 Privacy 63
5.4.2 Reliability 63
6 Chapter Discussion & conclusion 68
6.1 Proposed solution how to increase trust 68
Description of IDEMIX solution 68

6.3 Main Functions..... 71
6.4 TPM in E-voting 72
A framework for trust in E-voting 73
Conclusion..... 80
Βιβλιογραφια..... 81
Έντυπη 81
Διαδικτυακη 82

Abstract of the e-voting

Nowadays, electronic voting systems are among the most security critical distributed systems. So different trust concepts may be are applied to mitigate the risk of conspiracies endangering security properties. These concepts render systems often very complex and users/clients no longer recognize whom they need to trust (what entity is for) . According to recent events, specific trust considerations are necessary to support users. Recently, more specific terms have been proposed in order to express, which entities can violate the addressed security properties in particular by illegal collaborations. Also it has to be inferred about how successful attacks can be missed. Based on this approach, it will be created a framework to formally and automatically apply these terms.

The introduced framework is applied to deduce previously manually derived resilience of some of different kind of e voting systems. Additionally, in this work we can access to some more trust issues about the e-voting infrastructure.



Introduction

Recently, the interest has been increased in electronic voting systems and will be increase more and more in the near future. There is also interesting with voting machines as well as remote Internet voting schemes & structures. In this paper, it justbe considered Internet voting schemes and it is being used the term electronic voting or e-voting interchangeably. Electronic voting schemes are complex distributed systems with particularly strict security requirements due to the nature of elections. The upper statement varies from election to election.

Many of analysis and verification techniques for electronic voting have been introduced over the past. The Common Criteria, in particular the Protection Profile for electronic voting, is an international standard for security evaluation, which has been successfully applied to electronic voting schemes. Additionally, many researchers evaluated proposed voting schemes, both with formal methods and by cryptographic means it will be shown at next. However, these techniques mainly investigate external attacks (e.g denial of service and do not address illegal collaborations between different entities).

However, specific considerations about the trust are necessary because the implemented trust concepts result in very complex systems such as are the distributed systems and voters are faced with the problem whom to trust not to illegally collaborate with other entities. According to Volkamer et al. propose resilience terms to derive which entities are to be trusted and them not to collaborate maliciously in order to ensure security properties. Another thing that would be important is to express how robust a system is behavioral against conspiracies of entities that do not behave in a good manner.

1 Chapter Meanings

1.1 What is E-voting?

With this term there will be different opinions in which case in order to avoid havoc we should take a look further. E-voting enables voters to cast a (secure and secret) ballot over the Internet or an Intranet (in the case we have internal elections or decision making), while some reports/ authors distinguish the terms e-voting and voting in a remotely manner. A key element is the remote vote casting nature of the procedure. Another important thing is the need for computing equipment (resources hardware available), as well as for communication means for a citizen to exercise his or her voting right (http://www.e-voting.cc/en/it-elections/definitions/).

1.1.1 Paper Voting (Classical elections)

Traditional paper based voting can be time consuming and inconvenient. E-voting not only accelerates the whole process, but makes it less expensive and more comfortable for the voters and the authorities as well. It also, reduces the chances of the errors, E-voting system should provide all basic features that conventional voting does, further should furnish more services in order to make the process more trusted and secure.

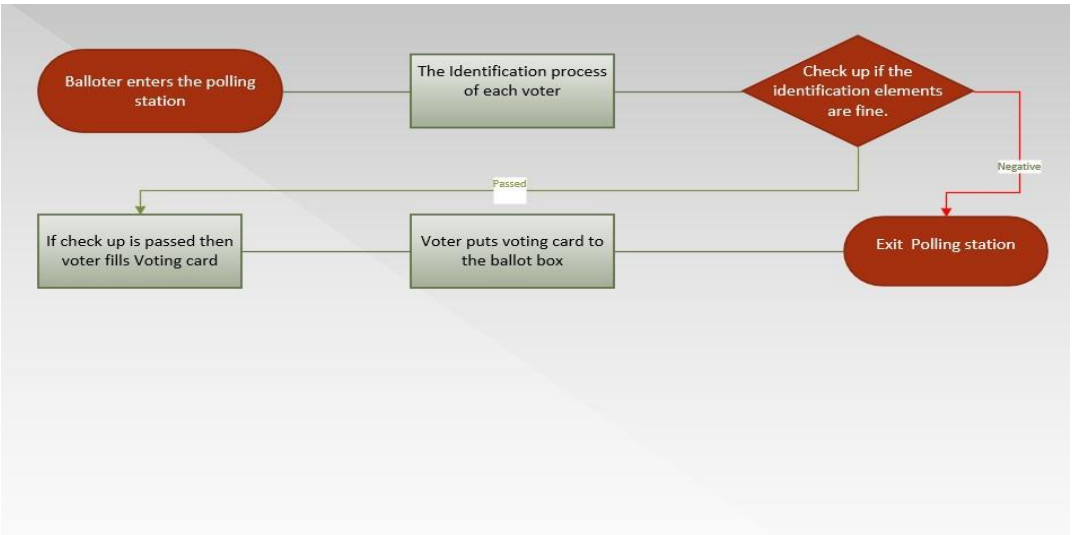


Figure 1 Diagram of classical voting

1.1.2 Description of the e-voting system

E-voting has similar qualities with classic paper voting system. In classical paper voting elections process voters are entering the polling station and have to be identified.

If identification is right the voter is able to vote .The whole scenario can be seen in the picture above. Nowadays, we have two different categories of e-voting systems. And these are first the voting process in site / platform of the e-voting system and second e-voting remotely.

In the secondary option (remote e-vote) voters have the opportunity to vote by using computers systems at remote locations or at polling stations inside .So citizens use computers and networks for electronic voting process. Voters can vote either internally or externally (from abroad).

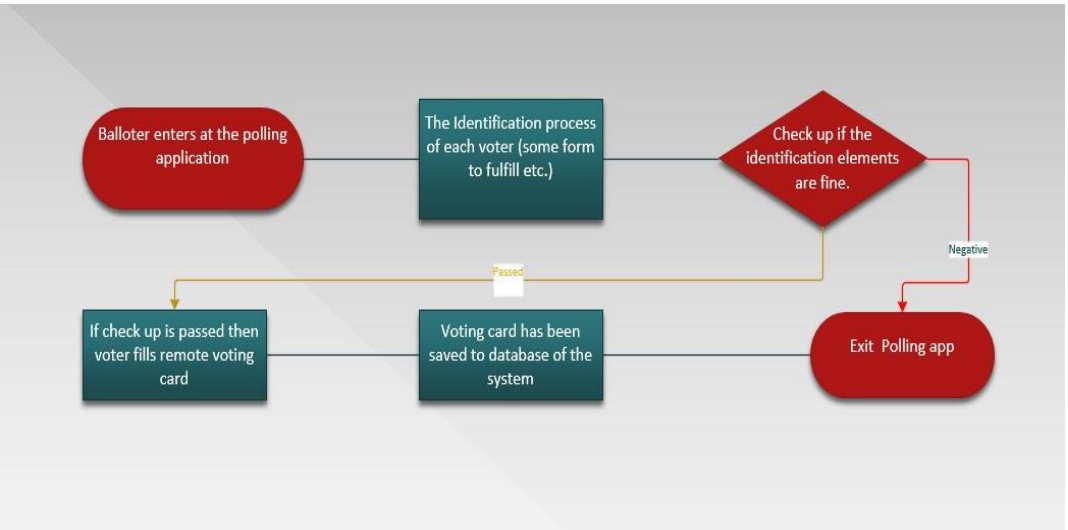


Figure 2 Diagram of e-vote

1.2 Definition E-vote

The type of e-voting that has been characterized by two features: the user can cast a ballot remotely over the Internet (WWW) and during more than a few hours on or prior to voting day without supervision of official authorities. In this definition has been useda source from (Alvarez, Hall, and Tracheal (2009, 497)) who state that what

is revolutionary with Internet voting is that the ballots can be cast remotely via the Internet connectivity. This definition explicitly excludes the different systems of electronic voting that are based on direct recording machines (DRAM) that replace the traditional ballot box and are basically intended to make the election process more efficient and less expensive.

Definition: In general, an e-voting system means an entirely automated electronic voting environment which enables remote voting for every citizen who wants participating at election process. This system eliminates manual registration verification, facilitates monitoring, voting, and tallying procedure. Furthermore, gives accurate and immediate result (Sang OK Ch oi & Kim, Journal of Information Technology, 2012) .One important finding which includes user interaction from preexisting established analysis is that interestingly, it turns out that accuracy indirectly influences user intention to use the e-voting system through perceived usefulness, while its direct impact is not statistically significant. Another hypothesis in the paper (Sang OK Ch oi & Kim, Journal of Information Technology, 2012) is how the influence of confidentiality is consistent with the literature.

Internet voting systems are usually grouped into three general categories: poll site, kiosk and remotely manner.

Poll site: This manner of voting systems requires voters to go to staffed polling sites and use computer machines to cast their electric votes. A network (Internet or private) is used to transfer ballots from each polling place to a centralized site, where votes are tallied and election results are published.

Kiosk: This type of system allows voters to cast from computers/ATM- looked like machines situated within kiosks. The kiosks are installed by the voting authority in suitable locations such as post offices or shopping malls and connected to a central location via the Internet LAN (or a private network). A vote that is going too inserted at the kiosk will immediately be forwarded across the network to the centralized tallying site. Once the voting period for a given election is up, the associated tallying site publishes the result of that election (http://www.e-voting.cc/en/it-elections/definitions/).

1.2.1 Definition of trusted system (E-voting)

In the e-voting content, the system must guarantee that stored information is not disclosed to anyone without proper access, and that voting information is not modified by unauthorized parties either authorities. It is important to imply that analyzing what trusted authorities are and what measurement is existing to see if there are trusted third parties on e-voting process. As it is important to verify security principles in the voting process stages, e-voting system is considered to be a trusted system but in this paper you have to define also management of trust framework so the clients have to obtain trust to the system concurrently.

1.3 Classification of e-voting

1.3.1 Polling station

The department can provide the reliable without virus, and easy handled voting machine in the polling places. The voters can be authenticated by the traditional protocol & mechanisms of local institutions and the technological authentication of voters might not be necessary. It provides higher security compared to other electronic voting places.

1.3.2 Home with voter's computer

Voters can cast their ballots by using their own devices at home. It is hard to prevent the third party's advertisement appearing on the screen while voting. It is much more difficult to secure the voter's computer from the attacks of hackers and virus 'because each voter sometimes is a simple user and that seems to be very negotiating issue. In contrast to the upper, remote Internet voting changes the act of voting in a cardinal way. The fact that votes can be cast remotely from almost everywhere and that the voting process could be integrated in the daily online routine creates the revolutionary potential of this new way of voting. E-voting makes it easier for people to participate in an official election because the voting act can be done from everywhere on the road. However, there are concerns about this kind of electronic voting that are not only related to security issues but also to the fact that transferring a public act into a private setting may change the way public elections are perceived by individuals and the very nature of the election process .

1.3.3 Voting with mobile devices

The voters can use their devices to get access to Internet in any place and cast a vote through the electronic voting system. Not only can the laptop be used to vote, the PDA, cell phone, and any other mobile devices might also be used to vote in the future. But there are many harsh problems need to overcome. The security is the most serious problem. It is vital to make sure that the computerand network in which h the voters get access is not monitored, intercepted, or tampered by any attackers.

1.4 E-voting in controlled or uncontrolled environment

E-voting in controlled environments occurs when the casting of votes takes place in polling stations either polling kiosks or other locations under the oversight of personnel appointed by the electoral management body (EMB). By that means the election administration process can to a great extent control the voting technology as well as the procedures and conditions under which voters are casting their ballots. E-voting in controlled environments can be analyzed as the electronic equivalent of Traditional paper based voting in polling stations.

On the other hand, e-voting in uncontrolled environment occurs without any oversight and from voting devices cannot be managed by any election admin. In uncontrolled environment there are issues such as privacy of the ballot, intimidation, vote – buying, impact of digital bifurcate, technical integrity of the devices from which the votes coming from (IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf, policy paper, 2011).

1.4.1 Voting Entities

Authority: Denoted by A, is responsible for issuing the keying material, i.e., the encrypted credential and the candidate slate (Ballot) to the voters.

- Voter PC: Here is the voting client application.
- Authentication service: Sends the ballot-er credentials to the client's PC.
- Vote Collector: This is the machine that stores the encrypted votes.

- Validator: Denoted by D, is responsible for the validation of all votes cast. This actor participate more at tallying stage and verification process.
- Talliers: The set of nT Talliers, denoted by T, are responsible for mixing the ballots, jointly counting the votes and publishing the final tally. Votesate-voting system are mixing by mix nets servers who are responsible for shuffling process.
- Voters: The set of nV voters, denoted by V, are the entities participating in the elections classical, local or European.

The Authority, Validator and Tallier are a set of entities, jointly performing the responsibilities. This is to eliminate dishonest entities. If at least one member of an entity from the set is honest, then no bad activity can be done to votes (http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/aegean/paper6.pdf).

Figure 3 SWOT

In general, in the upper scheme we see hypothetical strengths & weaknesses of e-voting systems.

1.5 Technology Problems in E-voting system and problems identification

As it is known for a long time that e-voting systems were developed to make voting more easily accessible for all the people who are citizens and to boost voters' confidence & trust at the election process. Other aspects that have boosted by e governance policy would be security, robustness, and privacy issues which remain big challenges until today. At first, computer security specialists have identified security problems in e-voting technology systems (Reference to: Kohno, Stubblefield, Rubin, & Wallach, 2004; Perrow, 2007; Schneider, 1993, 2003). Kohno et al. (2004) found critical security problems that encumber e-voting system such as unauthorized privilege escalation, poor cryptography (misuse of cryptography), vulnerabilities to network threats, and dangerous practices at software engineering. The main research concern from the idle of security perspective has been the development of robustness, reliability, and security at e-voting systems (TadayoshiKohno , Analysis of electronic voting system, 2004).

From political aspect of view, political science academics argue about how big impact of e-voting has on enhanced democracy. Some of them are (Dawes, 2008; Fountain, 2003; Hilbert, 2009; Moynihan, 2004; Thomas &Streib, 2003), the digital divide (Alvarez &Nagler, 2001; Lazarus &Mora, 2000), transparency and privacy (Gumbel, 2003), and administrative and social cost savings (Edmiston, 2003). They recognize both the prospects and challenges of voting, and they examine how we might overcome the vulnerabilities / threats of the e-voting system (technical manner) and enhance representative e-democracy with less costs and higher voter attendance percentage. Many researchers such as are (Carter &Belanger, Yao and others) analyze e-voting system from information technology and behavioral (psychological) viewpoint. The debate process from this aspect of view has two main arguments [trustworthiness + compatibility in how to use e-voting system].

1.6 Functionalities of E-voting Systems

- Electronic voter lists and voter authentication. Part of an electronic voting system can be an electronic voter list, covering either a single polling station or the entire country at parliamentary elections. This list can be used to authenticate if eligible voters have casted and to record the ballots by them.
- Poll worker interfaces. Special functionalities that are only available to poll workers, for example, resetting the vote count at the opening of the polling station, closing polling.
- Interfaces for casting votes. These include touch screens, optical mark recognition (OMR) ballot papers that are fed into a scanner, touch sensitive tablets, push buttons, web pages (web application platform for e-voting) or special client software for Internet voting.

- Special interfaces for handicapped voters. These include Braille or audio input devices for the blind, easier access for voters with physical disabilities, and simpler GUI for illiterate voters. One of the advantages electronic voting that has is giving access to anyone in relation to classical elections in which is more restricted.
- Interfaces for the results output. For voting machines (see the definition below) this is often a printer. However, some machines only use digital displays. Once voting is closed this interface can be used to display or print the results that were recorded by the voting machine. If results are printed the printouts can be used as physical evidence of the results produced by the voting machine, and copies can be distributed to stakeholders present at the polling station and can also be posted forpublic display (Melanie Volkamer , Evaluation of electronic voting system ,2009) .
- Printers for printing a voter-verifiable receipt for each vote (see below on the voter verified audit paper trail, VVPAT).
- Result transmission system. Many voting machines can transmit results to central counting systems, for example via the Internet, telephone, mobile phone or satellite connection. In the absence of communication links, the

results can also be transported physically, using electronic storage media such as memory cards.

- Result tabulation systems, usually located at result processing centers. At the end of Election Day, they receive electronic results from polling stations and automatically tabulate the results for the various competitions and districts.
- Result publication systems. Preliminary and final results can be published in many different ways including on websites, Cd's, and geographic visualization systems, and if required on all levels of detail down to single polling stations. The more detailed the published results are, the more transparent the election.
- Confirmation code systems. Some e-voting solutions allow for control codes that are intended to allow individual verification of each vote by the relevant voter.

1.6.1 E-voting without independent evidence of ballots casting

Nowadays, e-voting systems in controlled environments output physical evidence of the vote cast in the form of paper receipts for every voter (often referred to as VVPAT) it looks like a receipt when you purchasing a product . Voters can verify that they vote just looking at the receipt and then deposit the receipt in a ballot box. By manually re-counting the receipts, the results presented by the voting system can be independently verified by an authority. The results of an entire election can be verified by a well-designed manual recount of receipts from a random sample of polling stations. E-voting systemsin uncontrolled environments commonly do not produce physical evidence as these could be used for vote selling or manipulation either. Additionally, as the voter would keep the receipt, a manual recount is not possible, which renders such receipts useless. However, some Internet voting systems utilize a return code system that allows voters to verify that their vote was received none modified by the counting server.

If e-voting systems provide no physical evidence of the votes cast, direct verification of results is not exist. Theresults produced by such a system can only be indirectly verified. Indirect verification relies exclusively on a strict certification process against agreed standards in combination with tight security measures that prevent any

violation of the voting system's integrity. In these circumstances it can be difficult to communicate the reliability and trustworthiness of the e-voting system in a transparent way to a critical or non pro audience (voters) . This might become a big challenge in a context where the EMB does not enjoy the full trust of the electoral stakeholders. There are end to end voting systems that are using direct verification but there will be much more difficult to pursue voters to use it for election process because this system is destined for more professional level which more simple people cannot having so trust would be weakened (IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf, policy paper, 2011).

1.7 Description of EVS technologies

An Electronic Voting System is an entirely automated electronic voting environment framework that enables remote voting, eliminates manual registration verification in paper, enabling monitoring, voting and tallying, and lend to accurate and immediate results. An EVS means a web-based EVS which allows balloters to participate in elections wherever they have access to the Internet (Allers, M. A., &Kooreman, P., More evidence of the effects of voting technology on election outcomes,*Public Choice*, *139*, 159–170, 2009).

Table 1 Relationship between voting requirements and systems

Requirement	Description	PVBS	**PEVS**	**REVS**
Authenticity	Only persons with the right to vote should be able to cast a vote	+/-	+	+/-
Singularity	Each voter should be able to vote only once	+	+	+
Anonymity	It should not be possible to associate a vote to a voter	+	+	-
Integrity	Votes should not be able to be modified or destroyed	+	+	-
Uncoercibity	No voter should be able to prove the vote that has cast	+/-	+/-	-
Verifiability	Anyone should be able to independently verify that all votes have been correctly counted	+	+	-
Audit ability	Voting systems should be able to be tested, audited and certifiable by independent agents	+	+	+
Mobility	Voting systems should not restrict the voting place	-	-	+
Accuracy	Voting systems should be clear and transmit accuracy, precision, and security to voters	+	+	+
Availability	Voting systems should be always available during the voting period	+	+	-
Accessibility	Voting systems should be accessible by people with special needs and without requiring specific equipment or abilities	+	+	+/-
Detect-ability	Voting systems should detect errors, faults and attacks	+	+/-	+/-

In the needs of explanation here, two main categories of e-voting schemes are compared .These are PEVS (polling site e-voting) & REVS (when you cast your ballot in remotely manner.

1.8 Practical Cases (Proposed systems)

One of the earlier proposals for remote Internet voting system was the secure voting in Symposiums (SVIS) voting system, by Sako in 2001. This system was useful for selecting the best dissertation in workshops and symposia. SVIS collects encrypted votes and uses efficient mixing before the final tally. It was a mix net based remote voting system, meant for a small electorate. Hence the security provisions were limited, making it not suitable for a real time election. The system did not address the problems of improper influence, and has not introduced malware analysis too.

The secure electronic registration and voting experiment voting system (SERVE) , an Internet based system, was built for the U.S. Department of Defense's Federal Voting Assistance Program (FVAP). The SERVE had many vulnerabilities and the project was subsequently discontinued. The major criticism against SERVE was that the Web server recorded the vote but the voter's ID was recorded too. If the Web server had been compromised, then the voter privacy would have been invaded completely.

Adder is an Internet based e-voting system developed by Kiayias et al. at the University of Connecticut. It is based on homomorphic encryption and free software released under the GNU GPL. This is a fully functional e-voting platform where the voter creates his/her encrypted vote which has the security properties such as robustness, trust distribution, ballot privacy, audit-ability and partial verifiability. But the proposed model does not address the issues such as vote buying and selling, coercion resistance, voter verifiability, malware and other things.

Civitas was another remote Internet voting system developed at Cornell University by Clarkson et al. This was an extension of the voting system proposed by Catalano et al. that uses both re-encryption mix nets and homomorphic encryption. Civitas was claimed to be the first electronic voting system with coercion resistant remote Internet voting. It was also the first system implemented to guard against unauthorized access. On the other side of the coin, the tabulation and verification processes were very slow, and no there was no provision against malware tool-kits.

Helios was proposed by Adida as the first open auditable web based voting system. It was a web implementation of the Tuinstra and Benaloh challenge voting system, similar to the Adder voting system. The major difference between the two is that in

Helios, the encryption of vote is done by the election authority; Where as in Adder, it is done by the voter. Helios was meant for the elections of small online electoral communities. In spite of the easiness in use, speed and open source nature, it was not suitable for a major election. (Adida B Helios: Web-based open audit voting,Fourteenth USENIX security symposium (USENIX Security , July 2008).

1.8.1 UK pilot

In 2002, 30 pilot areas in the UK carried out municipal elections using innovative technologies. The goals of the pilot projects were to encourage participation in the elections, to increase the diversity of voting methods, to improve the efficiency of vote counting and to increase the information available to voters (The Electoral Commission 2002). The projects were embedded in so called electoral pilot schemes, a program which seeks to technically update and improve the election processes in the UK.

Under the representation of the People Act 2000, local authorities in England and Wales can submit proposals to the Secretary of State for Justice to carry out electoral pilot schemes. Since 2000, a broad range of local authorities in the UK has applied to take part in the program. Every pilot that has been conducted was observed by the Electoral Commission, which is an independent public body with the duty to oversee and analyze elections. Their published evaluation reports are useful sources for the analysis of the different technologies being used. Due to these trials and the activities within this programme, the UK is often stated as being a pioneer on the road to electoral innovations.

In the 2002 election Internet voting was introduced as an alternative voting method within the 30 selected areas besides other innovations such as electronic counting, voting over precinct based touch-screen machines, over text messaging systems, via the telephone or with interactive digital television services. Of all eligible voters on that date, approximately 2.7 million people were eligible to vote in the 30 pilot areas, which represents about 7.4% of the electorate.

Different localities emphasized different aspects in their pilots, some tested all-postal voting, some concentrated on e-counting, others on Internet voting. St. Albans, Swinton, Liverpool, Sheffield and Crewe were the five local authorities that tested Internet voting as one element of a multi-channel voting approach. Each of them used slightly different voting procedures; However the common principle concerning identification was a combination of PIN and password (Will 2002, 53ff.).

An analysis of Internet turnout rates and overall turnout rates of the 2002 local elections revealed that Internet voting could not contribute to an increase in turnout. On average, 14.6% of the voters used Internet voting. However, these participants would have voted anyway, but this time chose to cast their vote over the Internet. As a result, remote electronic voting in the UK pilot schemes in 2002 expanded citizen choice, but did not increase the overall turnout.

Pilot schemes including online voting were held for the last time in 2007. In the analysis of this election, the Electoral Commission criticized the lack of a comprehensive modernization strategy and the fact that security risks in the e-voting process were not predictable. Also, the lack of transparency was criticized. Further testing of e-voting systems from private suppliers was recommended before they were utilized the next time.

1.8.2 Switzerland

A very prominent example of level-2-voting is Switzerland. This is due to the fact that there are many elections every year on different political levels, and that referenda play an important role in Switzerland. In order to pursue the goal of bringing forward e-participation, e-information and communication, the Federal Council of Switzerland launched three pilot projects in cooperation with the regional units (cantons) Geneva, Neuchâtel and Zurich in 2004 and 2005. Since then, a gradually growing number of communities of different cantons were included. The pilot projects are embedded in the "Strategy for an Information Society in Switzerland" which was adopted in 1998 from the Federal Council, and updated in 2006. Two elements of this strategy are worthwhile mentioning: The first is the "Guichetvirtuel", which is an online portal that was set up in order to inform about administrative activities. Second, the "vote electronique", which should enable people to vote or sign petitions over the Internet.

The long-termobjective of the initiative, that also envisions a series of e-voting pilot projects, is a nationwide introduction of Internet voting. The fact that Switzerland holds elections and referenda on several levels, the local, regional and national, describes a challenge as well as a chance: first of all a challenge, because for electronic voting, the different requirements of the political entities need to be met. But it is also a chance to try out different systems and approaches. Pilot projects on a cantonal level are therefore seen as an important step to test the introduction of e-voting on the federal level. It is being discussed as an additional voting method next to voting by mail and voting at the polling station. The main reasons for pursuing e-voting projects in Switzerland are to facilitate voting for Swiss people living abroad and disabled people, furthermore, due to the high frequency of elections and referenda, to speed up vote counting.

The three cantons that were involved in the first e-voting projects, Geneva, Neuchâtel and Zurich, used different systems due to different requirements. For example, Geneva seems to be ideally suited for e-voting experiments since it is the only canton that already operates a centralized voter registry.

2 Chapter Infrastructure of electronic voting system

2.1 Infrastructure of E-voting system

As a general perspective e-voting system includes three stages that are shown above:

- Pre voting stage (I)
- Voting stage (II)
- Post voting stage (III)

Considering E-voting systems this way follows the high level models of election systems given by The Organization for the Advancement of Structured Information Standards (OASIS). The OASIS consortium specifies a so called Election Markup Language (EML) especially for the exchange of data within E-voting processes.

2.1.1 Pre voting stage

There might be various ways to become validated as a candidate to be elected depending on the region legislation and rules nomenclature. A candidate has to meet some legal restrictions.

In continuously, nomination process results in a list containing all the upcoming candidates, the so called candidate list. Additionally, the model (EML) includes the referendum options nomination process in parallel to the candidate nomination process. In principle, they are quite similar beside the differentlegislative restrictions. Even the options nomination process leads to a resulting options list.

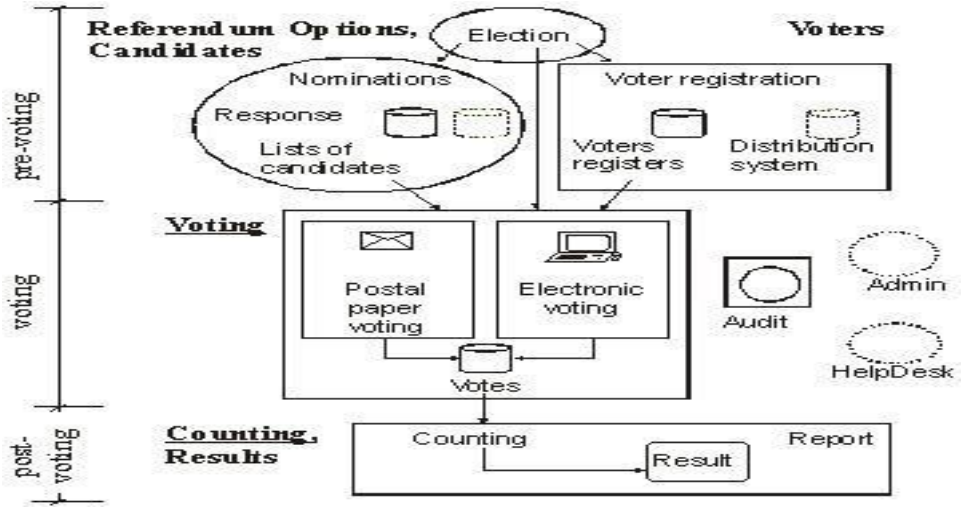


Figure 4 Pre voting stage scheme

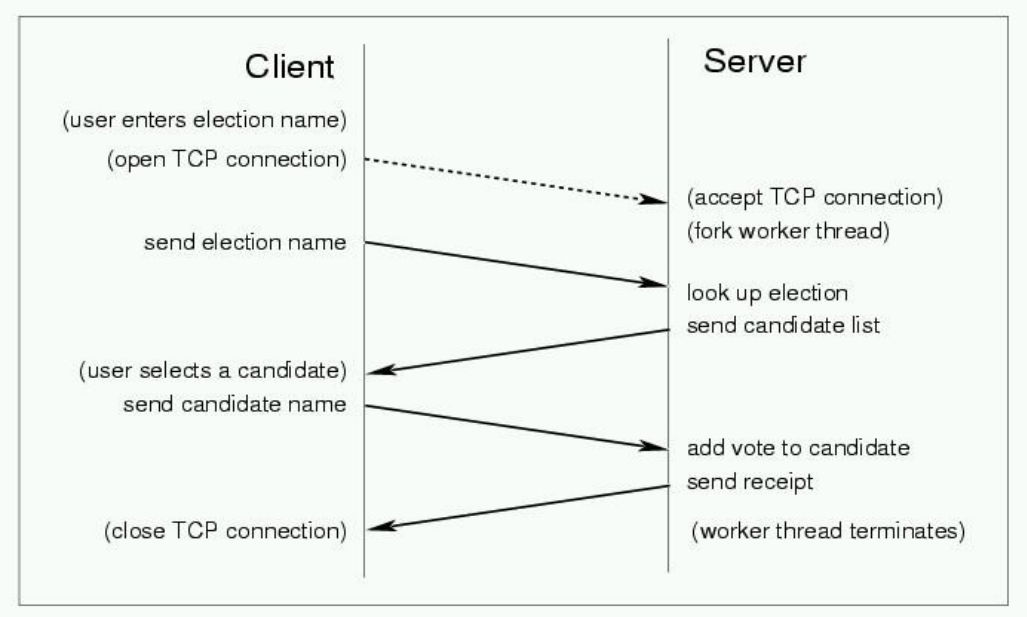
2.1.2 Registration process

Depending on the regulations each voter has to register for voting explicitly. On the other hand, in many countries citizens are registered for voting automatically. However, the outcome of this process is an election list containing all persons allowed to vote.

2.1.3 Voting stage concept

Depending on the results of the pre-voting phase the voting stage enables all eligible voters to make their decisions and cast their votes. By the use of the election list the voter has to authenticate himself/ herself as an eligible voter and has to cast his personal vote.

Since the voter might have an alternative to E-voting application and since conventional voting with paper ballots must be provided in parallel universe, the model has to consider multiple possibilities (R.Aditya ,Colin Boyd & Ed Dawson , Implementation issues in secure E-voting schemes, Queensland University of technology, 2004) .



Εικόνα 1 Client - Server communication

2.1.4 Post stage

In particular this phase covers counting process and result reporting mainly.

- **Countingprocess**: Counting is one of the most critical steps. Here, the possibility of recounting must be considered as an important part. Counting has to be remunerable and the input such as the cast votes in particular, has to be putted into archive.
- **Outcome**: Here an analysis system is needed. Such a system provides the auditing team and the election officials with reports. One of the most significant reports is the final result of the counting. There is no need to speak for this that time.
- **Audit Administration process**: Beside the stages and roles given above, there are some other important actors and components in the system. Very important are the audit mechanisms needed along all stages of the election process. On the first hand, it is important to have possibilities to prove the correctness of the process as such. On the other hand, it is crucial to do not violate the main principles and security requirements, keeping a vote a secret thing. Finally, auditing is necessary to prove the authenticity of the outcome of the election.

System administration is playing major role since administrators are allowed to have permission access to the system. Nevertheless, administration is needy and except that

the security concept of the E-voting system has to protect crucial personal data and components, the secrecy of the ballots in particular.. Not only technical security mechanisms are qualified for the above and can guarantee this but also the administrative personnel has to be elected in respect to reliability as an idea.

2.2 Cryptographic scheme's

Randomized Token:

It's a simple and no cryptographic solution and is based on anonymous token id's which have the role to protect election secrecy. The ballot-er uses this generated tokens to authenticate himself/herself as an eligible user without the e-voting system knowing his true identity.

Blind Signatures:

The concept of theses cryptographic protocol was firstly introduced from Chaum(1982) which authenticates a message digitally without having known the real message . This protocol 'feature' provides the system with unlink ability. Electronic blind signatures have like the same role as the physical blind have.

Physical are related to the envelope so something secret is on the white paper, next the carbon is placed on top of the paper and the envelope it is sealed. The validator signs the envelope! The signer doesn't know the content of the signed document but knows that his signature is on this (K.MacNamara& I.Iedemska, A survey of Electronic Voting schemes , 2012).

Full Blind Signature:

Process:

- Alice takes the document and multiplies it with a random bit (value). This random is known as the blinding factor.
- Alice sends the document to the receiver Bob.
- Bob signs the blinded document.
- Alice takes off the blinding factor leaving the original document signed by Bob.

This protocol feature doesn't give permissions to Bob to see the contents of this document. If the multiplier factor is random truly then Bob cannot see the contents.

Or viewing the document. If there is one chance Bob has the signed document with his signature on it after the steps have completed, there is no possibility for him to prove to himself that it is the document that he signed on (K.MacNamara & I.Iedemska, A survey of Electronic Voting schemes , 2012).

Properties:

Bobs signature is valid. The signature itself means that Bob is the signer.

It will be convincing Bob that he has signed the document if ever show to him.

If even he knows every possible blind signature makes him not determining when he signed the particular document.

Some who is in the middle and watch the protocol, has a less access to the information than Bob has.

2.2.1 Categories:

Blind e-ballots: Each voter encrypts his votes and sends them to the validator.

The validator checks if the voter is eligible. The validator also signs the encrypted document with blindly behavior .The voter unblinds the receiving 'c' and gets a signed e-vote which is sending to tallier. The responsible authority knows that e-ballot was came from eligible voter because it is signed first from the validator, but doesn't knows voters identity.

Blind tokens: The voter sends an anonymous token instead of blinded e-vote to the validator, with some identification and authentication data. After, he receiving a digital signature form validator on this blind token. The voter calculates the value form the signed authentication token and sends the datasimultaneously with e-vote to the tallier. The acceptance is the last step because the e-vote has the digital signature.

2.3 Categories of cryptography at e-vote

The process of e-voting at different stages until the end can be done usually with Two main schemes which are in most use:

1) **Homomorphic Tallying**
2) **Mix networks**

The Homomorphic encryption is one of the two basic structures for electronic voting protocols, which has an interesting attribute.

In case multiplication for the cipher texts (the votes in this case) and the result comes out, which must be deciphered, this will occur after the decryption process will be the same that someone had to decrypt all messages (votes) altogether and would be summed together. It appears that this property is very useful in an electronic voting algorithm.

$$E(x) \otimes E(y) = E(x \oplus y) \Rightarrow \prod_i^n E(b_i) = E(\sum_i^n b_i) \quad (1)$$

In such a system, each voter encrypts his vote with zero or one for each candidate in the electoral process list. In this category we are not interested in the "non-binding" of the encrypted vote with a voter. Additionally, the votes can be accumulated in a public bulletin board and anyone can verify that his vote has been accepted, or that nobody voted twice.

When the upper process is completed, the procedure applies Homomorphic cryptography to get the product of encrypted votes, and then the product is decrypted.

The private decryption key is shared among a few that are reliable authorities that work only for decryption.

As long as at least one of the principles is reliable to trust it, individual votes cannot be decrypted before the end of the voting process.

The difficult part in such systems is how we make sure that an encrypted vote is really the encryption of value 0 or 1, and the encryption has not be done on something else. The protocols used in electronic voting based on homomorphic encryption, using non-interactivezero-knowledge proofs. In non-interactivezero-knowledge proofs need not interact recipient and controller (inspector). To confirm that an encrypted vote is really the encryption of 0 or 1 and is not encrypted into something else it is mandatory the contribution of the voter.

The voter prepares the plain-text (the vote in our case), which encrypts it using the homomorphic encryption algorithm. It also provides zero knowledge proofs. Namely that the contents of the encrypted vote is valid. After append his signature the ballot shows the real identity. Only votes that are signed by the electoral system, will be calculated at the end.

The encrypted vote, the evidence and the signature posted publicly on the bulletin board of the electoral process. In particular, the main drawback to homomorphic systems is that the algorithm will limit the form that has the plain-text itself (the vote). Typically can only number or some type bitmap. This makes sense in the case where we have a proliferation of ballots which would allow ballots have arbitrary content.

2.3.1 Mix Networks

In the Mix Networks are two main categories:

1) **Decrypting Mix nets**

2) **Re-encrypting Mix nets**

The basic use of Mix Networks is to make shuffle the votes that take as input to the outputs in a different order.

In this way, and since the mixing is done by many mix servers in a row, it becomes anonymous voting. So I do not know what vote corresponds to what voter. The Mix Server does not have to just do shuffle the votes. Should the cipher text votes in their entry, be different from the cipher text votes in their outing. Otherwise, one could fairly easily by looking at the cipher text in the input and output to understand the algorithm used for the shuffling.

The approach is based on the mix nets are easily understand because the sequence of cryptographic building much like how it appears as classical election process with using like paper voting in national elections :

First step: The voter prepares the plain-text (his vote) and encrypts it in such a way that only himself/herself can decrypt it. Also is using zero knowledge proofs to assure that the valid vote, will be counted.

Second Step: Then the voter confirms that he is the one who is applied to, after a check on the election committee, which checks whether the voter is entitled to vote or not. Also, the voter checks the zero knowledge proof to assure that the encrypted plaintext (vote in our case) contains only the valid vote and nothing else. If applicable the latter, said the Election Commission implements blind signature to encrypted vote. Finally, the committee will record that the voter has voted and so it seems that he can vote once a time.

Third Step: At voter's side is sent a ballot with signature coming from the e-vote system, vote for decrypting process. In the current situation, voter has the plain-text (vote) which has the bearing signature of the electoral committee. This shows what is meant by blind signatures: meaning that the Election Commission can sign the plain-text (the contents of the vote) even if it is encrypted. Now if encryption leaves the place the contents of the plain-text is still signed. At the end of the process of voting, only the votes signed counted at the end (Tallying).

Forth Step: At this stage the voter encrypts the vote of the public key used for this process. After sending the vote through a mix net network which anonymize votes. This mix net consists of a network of independent computer systems (machines), each of them somehow make transfers of votes that take as input and sends it to the next node in a different order (**shuffling**). Every link in mix net could also include its own encryption decryption system. The common point of all this is the anonymity of the vote - no one should be able to identify what the vote was originally cast by a voter.

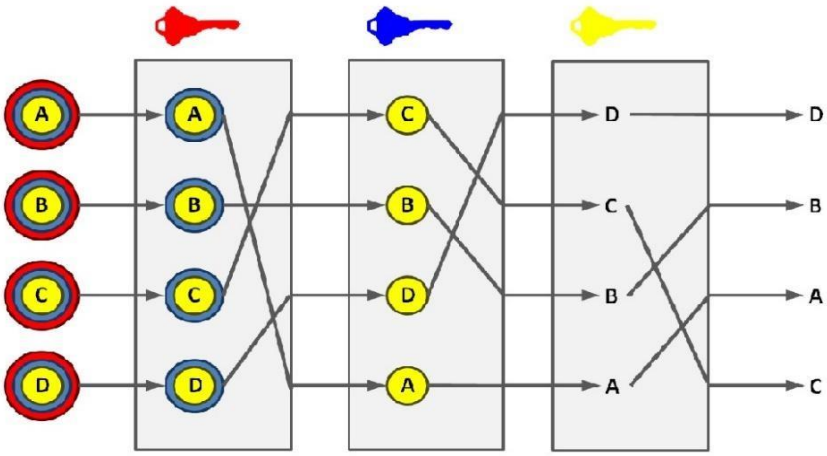


Figure 5 How mix-net works (general)

2.4 Threats (General idea)

E-voting systems threats exist in many variant of forms! So, they can compromise an E-voting system in many ways. Different threats can compromise the various areas of security leading to untrustworthy systems.

2.4.1 Denial of service Attacks (D.O.S)

Denial of Service (DoS) attacks that are put through have slight consequences and in most cases the extremely affect the ability to provide maybe availability to the system. Might be a slight chance to have different kind of attackers a hacker or an insider may compromise the availability to a voting system.

2.4.2 TCP death

The ping of death relies on a flow in some Transmission Control Protocol, Internet Protocol (TCP/IP) stack implementations. Technically, the attack relates on how to deal with unusually and illegally large ping packets. Remote systems receiving such kind of packets can crash as the memory allocated for storing packets overflows (this is buffer overflow attack). But attack like this does not affect all systems in the same manner because some systems will crash, and others will remain unaffected in some way. (Evans M. and Fumell S.,"Internet-Based Security Incidents and the Potential for False Alarms," *Electronic Networking Applicationsand Policy,* vol. 10, no. 3, pp. 238-245, 2000).

2.4.3 Packet malformation

Packet flooding exploits the fact that establishing a connection with the TCP protocol involves a three phase handshake between the systems. In a packet flooding attack, an attacking host sends many packets and does not respond with an acknowledgment to the receiving host. As the receiving host is waiting for more and more acknowledgments, the buffer queue will fill up. Ultimately, the receiving machine can no longer accept legitimate connections.

2.4.4 Virus

Computer virus is a computer program that can reproduce itself and may cause undesired effects in computers where it is active. To do its malicious work, the virus needs to be executing manually usually from simple users. Usually viruses are located\ together with other code that is likely, will be executed by a user. As long as the virus is active on the computer, it can copy itself to other files or disks when they are used. Viruses made could destroy E-voting systems. This could compromise the availability at election time forcing governments and institutions to perform re-elections (Evans M. and Fumell S.,"Internet-Based Security Incidents and the Potential for FalseAlarms," *ElectronicNetworking ApplicationsandPolicy,* vol. 10, no. 3, pp. 238-245, 2000).

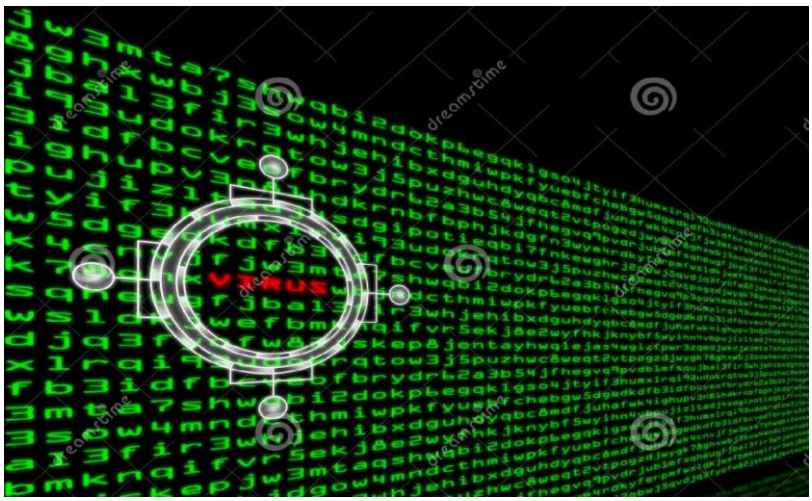


Figure 6 Virus 1

2.4.5 Trojan Horses

Trojan horses are parts of computer code that can be downloaded to a client's computer while connected to the Internet. They might be harmful from outside view, but it could possibly delete or modify an important file from the computer (example :Dll), place a harmful virus, or even steal user's cookies passwords when user submitted some form or did other activities .This makes all sorts of fraudulent schemes possible.

If the Trojan horse can access passwords, screen names and other personal information then can capture this confidential data and sent it to the attacker (especially in the e-voting system where the user submits the authentication code to the web platform of the system). Trojan horse represents an immense threat to systems confidentially and integrity of information of E-voting systems.

2.5 Physical Attacks in the E-voting

Many physical attacks can be carried out on E-voting system to sabotage or disrupt an election. Vandalism of E-voting systems would make themunavailable for the day of the election. Attackers could remove network connections and pull plugs out of E-voting systems causing votes to be lost somewhere. Attackers may remove hard drives/optical disks or smart cards replacing them with modified malicious data (with JavaScript code and other things). Voting machines could be stolen with attackers discovering sensitive voting information about users.

2.5.1 Unauthorized Access on e-voting

Since the system is Internet based, there may be a tendency for unauthorized people to access the voting system. This is prevented by the authentication mechanism using the biometric code of the voter, which is collected at the time of the initial in person registration of the voter with the Authority. The biometric code of the voter will be read by the application program and sent to the authority along with the other

information as a log file. This is matched with the original biometric code and the authenticity of the voter is established.

3 Methodology

3.1 Purpose of thesis

With this study it will be discussed with the method of literature review of any technical confidentiality between voter and vote and the system opportunity achieving new methods. Also, current technology and trust issues will be analyzed.

3.2 Methodology of research

About our research will follow theoretical approach and the kind of research methodology is qualitative. As for the techniques will be collecting data from literature sources, reputable articles in parables views and corresponding surveys. To most of the research consists of the systematic collection of information from already published sources.

The advantages of this method are that:

• allows the existence of theoretical responses literature

• has the possibility of partial adjustment,

• can go multiple conclusions,

• achieves moderate supervision

3. 3 Design

For proper design of the literature study and safe conclusions, the investigation will examine the following areas:

• Directions for proposals for confidentiality between the voter and the electronic system during the voting process

• The existing encryption methods and techniques that cover the problem of confidentiality.

• The overall theoretical background of the system of electronic voting.

• The trend is the study of resolving the question of confidence today.

3. 4 Results

The conclusion which emerges from the reading of this study is that it will highlight the main shortcomings of the system of electronic voting through the analysis of its operation and by reference confidence problems from the perspective of the voter. Finally, it designed a model of trust which will have particular subsystems in a large computer based system like E-Voting.

4 Chapter Confidence

4.1 Trust

Eventually, trust can be described as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trust or, irrespective of the ability to monitor or control that other party” (Mayer, R.C., Davis, J.H., Schoorman, F.D., An Integrative Model of Organizational Trust. Academy of Management Review 20(3), 709–734 (1995)). In a trust relationship there is an acceptance of vulnerability to a possible, but not expected, damaging action (Schlienger, T., Teufel, S., Information Security Culture: The socio-cultural dimension in information security management. In: Ghonaimy, A., El-Hadidi, M.T., Aslan,H.K. (eds.) Proceedings of the IFIP TC11 International Conference on Information Security, pp. 191– 202. Kluwer (2002)).
It is referred as different forms of trust in the literature relating to whether access is being provided to the trust-or's resources, the trustee is providing a service, trust concerns authentication or it is being delegated.

For example (When there are different options possible, such as in choosing a bank for one’s savings, a comparison needs to be made, and trust takes the place of confidence). Another practical explanation for trust in general is choosing to live in a high part of the Netherlands because as a person you have always lived there, so you have confidence & convenience for the safety of the place. If I choose to live in a high part because it may be less risky if sea levels rise, I have trust in it. In the former, the alternatives and the decision are implicit. In the latter, they are explicit.

A trust or trusts a trustee to use resources that he owns or controls them, which could be a software execution environment or an application software service. (Abrams and Joyce).

There is an obvious distinction between trusting an entity to read or write to a file on a server and trusting an entity to execute code within your workstation. Simple file access list requires that the trustee will follow the correct protocol rules, will not divulge information read, and will write only correct data (not invasive strategy). So If you allow an entity to execute code on your workstation needs a much higher level of trust. The code is expected not to vitiate the trust or's resources, to terminate within

reasonable finite time and not to exceed some predefined resource restrict with respect to memory (RAM), processor time, hard disk space, local file space.

Furthermore, resource access trust can formulate the basis for specifying authorization policy, which then is implemented into operating system (OS) or database access control mechanisms, firewall rules (IP tables) , distributed system such as is an e-voting system which includes a whole mindset of components . The trust relationship can be subtle into authorization policies that specify actions trustee must or can perform on the trust-or's resources .Consequently, trust is situational, its functioning is based on the ability topredict the behavior of the other and it typically emerges and builds up based on past experiences.

4.2 Layers of trust

The layers of trust view of the eVoting system is a view complementary to the other formal views and models of ordinary IT systems (e.g. business view, technical view etc.) and is employed in order to handle the complexity of the security issues related to e-Voting, as defined by its security requirements. This is so complicated that can be as high as the complexities that arising in other architectural views of such systems and the layers of trust approach can be used as a tool mechanism for managing these issues successfully.

The scope of the layers, and the correspondence to the e-voting system, is as follows:

1. **Scientific**soundness: All the components of the system should possess some type of security justification and be widely accepted by the scientific community. This layer corresponds to the selection of a cryptographically

Strong e-Voting protocol, based on provably secure cryptographic primitives, such as the El Gamal encryption scheme and zero knowledge proofs.

2. **Implementation** soundness: A methodology should be adopted that will lead to the verification of the implementation of the separate system components (e.g when you want to add a new hardware component to the whole system) as well as the system as a whole. In addition, such a verification methodology should be applied periodically to the system.

3. **Internaloperation:** The design and implementation should offer high availability and fault tolerance and should support system inspection, self-checking, and self-recovery plan from malfunction or a service maintenance break. The implementation of the cryptographically secure e-Voting protocol involves the use of proofs of correctness for all the executed steps.

4. **Externally visible operational soundness**: It should be possible for everyone to check logs and audit information at some level. The employed cryptographic protocol employs a number of publicly accessible bulletin boards where information is appended concerning the votes cast as well as the proof that the votes were taken into consideration for the computation of the vote outcome.

5. **Convincingthe public** (social context): It is important for the wide acceptance of the e-Voting system that the public will trust it when it in how operation process works on it. This trust can be, in general, amplified if the e-Voting authority publicizes the details of the design and operation of the e-Voting system to the public. There is a problematic issue for publicizing all the details of the system architecture and implementation as well as provide the software source code to the open space. In particular, in order to facilitate the system's wide acceptance, the first trials will be conducted on a voluntary basis with closed small groups or local associations, whose opinions can be easily gathered and analyzed (A.Antoniou, C.Korakas,...,A trust centered Approach for building e-voting systems, 2007).

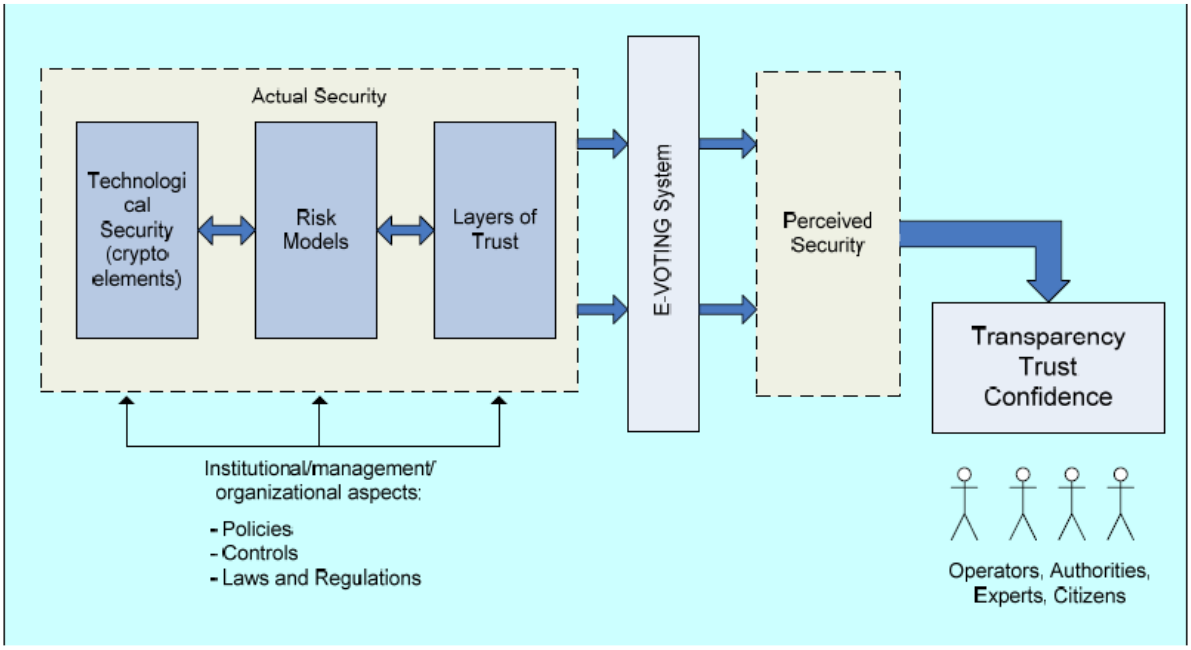


Figure 7 trust layers

4.2.1 Issues Influencing trust in e-voting system

In a more philosophical sense, as advanced by Latour (2005) in his actor network theory, a black box is something that has been inferred as 'black boxed'. A theory or technology of which the supporting network of act ants has become invisible. An act ant, according to Latour, is anything that participates in actions in a network of relations, and becomes what it is by means of the network. In the latter sense, other phenomena such as scientific theories or political systems can be characterized as black boxes as well. As there is no opportunity to discuss actor network theory in detail here, the important point to remember is that black boxes need not always be purely technological (IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf, policy paper, 2011). So according to the latter electronic voting machines are the black boxes as a conclusion.

Explanation-for-confidence is explanation that makes the user feel comfortable in using the system, by providing information on its external communications. Black boxes can be opened when trust is required instead of confidence; This opening produces an explanation-for-trust of how the system or network does what it is supposed to do; it reveals part of the inside workings, thereby reveals part of the risks, and thereby trades confidence for (possible) trust.

If the network can only reply to questions of justification, it can be considered a black box. In such a case, the network can only acquire confidence of the environment. Once trust is required, the black box needs to be opened in order to supply explanations for trust, in response to questions of transparency. In the latter case, the system thus needs to be designed in such a way that this is actually possible; This amounts to design for transparency.

Transparency is usually seen as the main goal, especially in e-voting, and it is considered essential for allowing the users to understand what the designers have done to protect them. Whether transparency also contributes to the security of the system itself is heavily debated: some would argue that makingthe protection mechanisms public will enhance the capabilities of the attackers, whereas other would argue that protection mechanisms can be improved by public scrutiny. In the latter case, explanations of what procedures are built into the design and what procedures exist if something goes wrong would then contribute to transparency (IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf, policy paper, 2011).

Example here for different alternatives in regions .In the UK e-voting pilots, multiple channels were offered to the voters, and they could decide themselves which one they wanted to use. In the Dutch system, the government needed to create confidence in the systems used, since citizens did not have the choice to go for an alternative option. In the British case, explanations of the systems could have the role of allowing citizens to choose, enabling trust rather than confidence.

Some of the issues that maybe influence trust at e-voting systems:

- Information availability and quality sessions about the system may influence voter's confidence in e-vote.
- The number of times electronic voting was used successfully may turn ballot-er confidence and trust in this kind of casting.
- The source code of the system if it is open free then voters may be some of them who have the knowledge can inspect the code itself this could be an advantage for electronic system.

- A significant issue is the variety of elections. There is a difference if we talk about topical elections or parliament either better European elections. In this issue maybe clients have different trust behavior in the system.
- Certification and auditing process may help clients/balloters to keep up confidence in e-voting.
- Another element which would be rational is who has developed & designed the system. Because of reputation sometimes that works forvoter's confidence (IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf, policy paper, 2011).
- Because there is a different kind of technology for e-voting up until now such as message voting with mobile and Digital television voting maybe a more secure & trusted system must be in use to gain the confidence by the public.

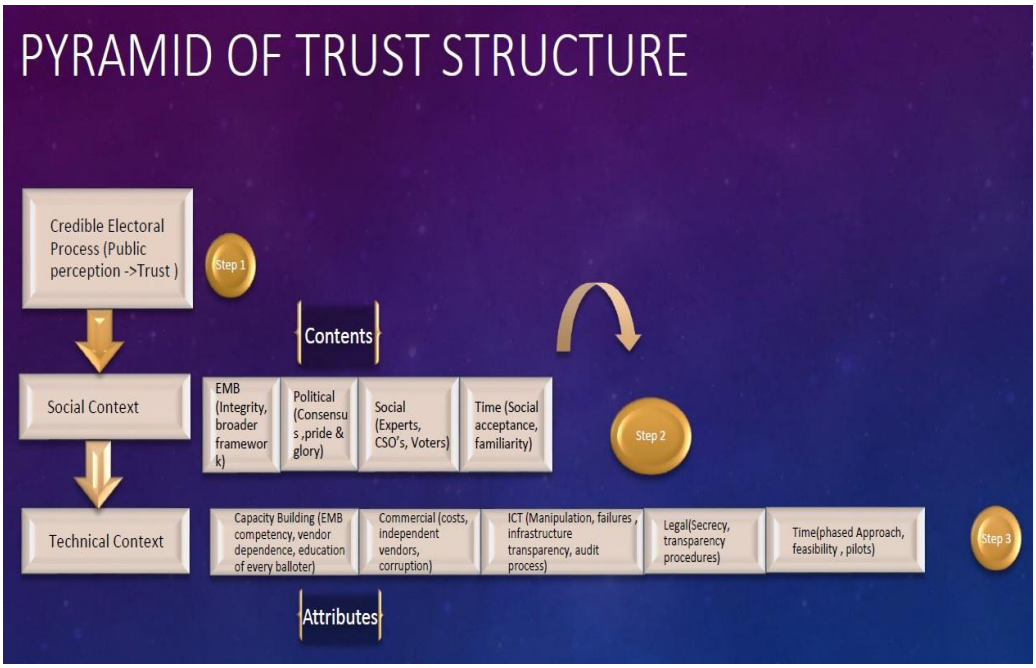


Figure 8 Pyramid of trust

4.2.2 Explanation of confidence (1)

In electronic voting, an explanation-for-confidence of the use of electronic voting machines is that they produce faster results. Or, alternatively, that they are more reliable and accurate than paper voting. Or, alternatively, that they have been tested by an accreditation organization. In such explanations, the black box of the system is not being opened. The primary goal is justification.

4.2.3 Trust view (2)

An **explanation-for-trust** would be an account of the measures that have been implemented to guarantee security. At the highest level of detail, the source code could be made available. The latter, of course, would not be an explanation for the general public, and may therefore not be sufficient to establish public trust in the system. The primary goal in such explanations is transparency.

4.2.4 Trust in e-voting process

On the other hand, trust is a hard to formalize concept that also raises philosophical and social (i.e. no engineering) concerns. For instance, Luhmann'sresearch considers trust as a mechanism which causes the reduction of complexity. Coleman distinguishes certain elements that define a trust situation between a trust or and a trustee. By definition a voting procedure is a trust situation, and in this case trust properties have to be reflected both on individual and system level, independently of the voluntary, custom/norm based, institutional or obtruded nature of the procedure. Trust is an emergent social property based on interactions between actors and for this reason, an e Voting procedure could, in principle, be established, if and only if, actors are convinced that it complies with certain trust properties (Luhmann, Niklas (2000) 'Familiarity, Confidence, Trust: Problems and Alternatives', in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, Department of Sociology, University of Oxford, chapter 6, pp. 94-107).

Public Perception

At the top of the level and the ultimate goal of electoral reform by implementing an e-voting scheme —is a credible electoral process that enjoys a high level of public trust and urges public to have confidence in the new system.

Public trust is initially mainly built on the socio-political context in which e-voting is introduced. Some factors in this context can be directly addressed by a comprehensive e-voting implementation strategy, while others, such as a general lack of trust in the EMB or fundamental technical opposition, will be more difficult to change directions.

A supportive socio-political context significantly helps the introduction of e-voting and can temporarily even cover up problems that may occur in the technical implementation structure. Trust in a solution that is technically weak can, however, be misleading (IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf, policy paper, 2011).

Weaknesses in the operational, technical or legal foundations will eventually occur and may then discredit not only e-voting system, but possibly the entire election process.

In case socio-political context is negative that would create serious repercussions, even if the technical and operational innovations of the e-voting solution are sounded well. It is very difficult to make e-voting systems transparent and their operations understood in the short and even medium term by a non-well educated public. Weak social and political support will wreak the havoc to the implementation of a trusted e-voting solution as opponents will find it much easier to disrupt trust in this voting technology by pointing to some of its deep weaknesses (McGaley, M. and Gibson, J.P., 'Electronic Voting: A Safety Critical System', National University of Ireland, Maynooth, 2003).

4.3 Social Content

E-voting tends to take a good deal of the responsibility for the electoral process away from thousands of polling station officials and place this responsibility in the central election administration and the implementers of the e-voting system. In doing so, the implementation of e-voting reduces the risk of widespread fraud and manipulation at polling station level, but concentrates the risk of manipulation at the central level.

Technically this could be beneficial in an environment where there is little public confidence in polling station officials, but where the central election administration authority is trusted. Furthermore, in an electoral environment where there is little trust in the central EMB structure, there is so much things which can be discussed about potential central manipulation.

As important as it may seems, maybe technology upgrade is another pro for every economy and law, the question will be if electronic voting systems could increase the existing capacity. However, if the initial capacity level is already low, the opposite is likely to happen: the positive effects are tend to fail and, if trust is already low, distrust is likely coming up (Estonia example : At 2007 the system was hacked but public acceptance gave another chance to technology upgrade) .

Together with the question of trust in the EMB itself, it is also important to consider trust in the broader electoral framework. In an environment where many stakeholders are not confident with the e-vote design, mechanisms to deal with electoral disputes and differences, officials or the government, the EMB will find it difficult to win the level of trust required to implement a widely accepted electronic voting framework.

Finally, to facilitate widespread social acceptance, the new voting technology needs to show particular benefits for voters. If voting gets easier, more accessible and more convenient for citizens they will accept and support the new system more easily.

4.3.1 Political Aspect

E-voting systems can be most easily introduced when there is political reason about the benefits of the new voting system. Political actors may, however, oppose at electronic voting for their own point of view, either in principle, because they have real technical concerns, or because they fear the new voting channel might be an advantage for their opponents? Or because they believe that other parties may receive more credit for designing better at this part of election? or just because they do not trust in the independence of those entitiesknown as third parties . Facing such opposition, successful confidence building may be difficult or is an unreachable dream.

4.3.2 Social context

Key social actors, such as(NGOs) and experts, often have strong opinions or concerns about e-voting. Ideally these actors should be included early on when planning the introduction of the system, both by providing them with practical information about the system envisaged and by allowing them to raise

Their concerns in the early phases of design, when there is still time to propose them. ICT security expert groups are often strong opponents of e-voting. Some of this opposition is quite fundamental, and many currently available systems do not address the concerns of such opponents. It is important to hear and address their opinions and clarify any misunderstandings, correct wrongs or accept certain risks as a trade-off for the benefits of introducing the new system. Also, non-technical opinions are important such as might be one which says that digital divide will be increased between affluent and literate people. Others argue that any spending on electronic voting is a luxury in such hard seasons where many citizens see their basic needs as not being catered for (political view).

4.3.3 Time

Time is a main factor on various levels. Operationally, e-voting cannot be introduced at one day, but social acceptance of it should realistically be expected to take much longer than pure technical implementation. Commonly it will take several electoral cycles without major technical glitches or political controversy, and with trusted results and civic education programs, before citizens and stakeholders are fully confident with usage of electronic voting, based on their own experience and knowledge.

Ideally, information and sensitization campaigns on the possible introduction of e-voting systems should start well in advance of technical implementation, with the possibility to shape the technical requirements of the system on the basis of the social context's response and concerns.

4.4 Categories of trust

4.4.1 Access Trust (Resource)

Jimmie is trusted to do Linux installations & upgrades and George is trusted to do NT installations on our section workstations.

- First year postgraduate and above students are trusted to use the e-voting platform for public elections & for academic purpose.
- I trust machines vote counters because they are reliable to the integrity of voter's decision.
- I distrust AB Garage so I will not take my car to be repaired there.

4.4.2 Provision Service by the trustee

The trust or trusts the trustee to provide a service that does not require access to the trustor's resources. Note this may not be valid in many services such as web services that download applets (plug ins) and cookies, and so do require access to resources owned by the trust or.Recently, in the domain of ASP's, trust is often an unstated implication of establishing a relationship, which is difficult to enforce or monitor it. The source code in mobile environment and mobile agent based applications obviously must trust the execution environment provided by the remote system (provision of service trust) but the execution environment should not be impaired by the mobile code (Lemuria Carter, Ronald Campbell, The impact of trust and Relative advantage on Internet Voting Diffusion, 2011).

Another form of service trust relates to issues as are reliability or integrityof the trustee. In E-Governance, the client voter trusts the vendor to support secure mechanisms that will ensure that passwords of lo-gin to platform for voting process are not divulged and to prevent transactions from being monitored or blackmailed. The vendor is also trusted to maintain the *privacy*of any information such as name, address, personal details about the voter (religion, political preference) which it holds in a repository about each client. There havebeen some high-profile incidents in the UK recently where this trust has been broken. Examples of this form of service trust are:

- Storing credentials of user preference in specific group of political idea inside the hard disk of vendor's resources every 3 hours for example.
- Trusting the voting machines system of vendor in which the credentials have been kept & saved.
- Trust e-voting platform Gui which is very useful for acceptance by clients huge percentage.

4.5 Certifications

This type of trust is based on certification of the trustworthiness of the trustee in our case the developer of the e-vote system by a third party entity, so "trust" would be based on a criteria relating to the set of certificates presented by the trustee to the trustor. Certificates are commonly used to authenticate identity (user ID) or membership of a group in Internet applications such as the registration e-voting for having the right to vote remotely for example. This may imply competence if the identity is a well-known enterprise. However, professional certification is a common technique used to indicate competence in the medical world, but in the e-government services is so underrated up until now.

To exemplify the upper issue we can infer about the certificates review of a client:

- When I lo-gin to e-vote system to see my status profile and submit my ballot preference I want to validate the URL by Verisign organization because is a known for trusted issues for this kind of services
- Another example could if each client have trust the authentication server when the client reach the specific domain of e-voting system.

**Here you need an external authority to be trusted by the majority of the voters.

4.5.1 Delegation trust

A trust or trusts a trustee to make decisions on its behalf, with respect to a resource or service that the trust or has ownership or controls. This is also called a special form of a trust decision-making service.

Ding and Peterson "illustrated a novel way of implementing delegation, with hierarchical delegation tokens. Their work relies heavily on cryptography. They propose a classification of delegation schemes, with appropriate protocols, which they analyze deep, based on efficiency(Lemuria Carter, Ronald Campbell, The impact of trust and Relative advantage on Internet Voting Diffusion, 2011). They also concentrate on access control". To exemplify the upper:

- If you trust the committee of voting process which is responsible to decide who has access to the database of platform of the user.
- Accepting anonymous authorization certificates for access to voter account issued by the www authorization service entity.

4.5.2 Infrastructure Trust

This refers to the base infrastructure that the trust or must trust (Deep down the hardware resources of the e-voting system). He should be able to trust the workstation, local network and local servers (in which the ballot-er submits his ballot) which may implement security or other services in order to protect the critical components of infrastructure.

It was recognized in early computing that in order to implement security known as the Trusted Computing Base (TCB) that had to be trusted by all applications & tasks executing on a machine to support the required security policy. The TCB can be viewed as the set of hardware, firmware (like bios version) and software elements, which are used to implement the reference validation mechanism . The TCB was seen as the basic component of a trusted computercontaining all of the system elements supporting the isolation of objects (code and data) on which the protection is based. It was destined at centralized systems preventing information flow to unauthorized users.

More recently the TCB has increased the bandwidth of its trusted components. To make the PC platform (servers and voting machines more trustworthy), an initiative was introduced to develop and formalize a trusted PC client and server framework.

4.6 Trust Management

There was one paper of the first to introduce the term trust management. Although prior security solutions for networked apps had an implicit notion of trust Management based on PGP or X.509 public-key certificates. Blaze defines trust management as "a unified approach to specifying and interpreting security policies, credentials, relationships which allow direct authorization of security-critical actions". They have implemented several automated trust management systems of note, namely: Policymaker /Key note/Referee. These are discussed in more detail in later chapters.

A common flaw with all these solutions is that they are used to identify a static form of trust that is when the programmer inserts code to evaluate trust more often at the start of a session. "However, trust changes with time. Typically a client ballot-er uses an unknown service provider (3rd part entity) with some trepidation but if the service provided is at great quality over a period of time, the clients trust in the service provider increases at some point". In order to handle the dynamic attribute of trust, solutions should have a notion of learning. They should be able to adjust to the changing conditions of the environment in which the trust decision was took place.

However, current solutions have no notion of conception to their own experiences (or that of others) in their decision-making process. These systems unconditionally accept credentials (user name | password) offered by the trustee (client) and then decide what the client is permitted to do or permission rights on the action in which he or she is doing. But, that may not be what the client currently wants to do. Even though there may be a relationship between the trust or and trustee, the trustee may wish to function in some other capacity than previously agreed upon. There is a need of negotiating the current relationship between trust or and trustee and the temperament at this.

Systems are changing in continuously manner and evolving so there is a need to (observe) trust relationships to determine whether the criteria on which they are based

still apply. This will also involve the process of keeping track backlog of the activities of the trustee and of taking the necessary action needed when the trustee has violated the trust or trust (agreement).

4.6.1 Trust Management solutions

Between trust or and trustee (ballot-er) there must be a trust policy language by some certification protocols to examine if the trustee is trustworthy.

A digital certificate is issued by a certification authority and verifies that a public key is owned by a particular entity. This CA does simply authenticate the owner's identity. This is necessary to establish connection in more detail a resource access or service provision trust relationship and may insinuated reduce the trust-or's danger to deal with the trustee. On top of that, the policy governing what resources or services the trustee is permitted to access is not handled by the certificate infrastructure, but is left up to the application process or layer by its own. Two of the main certificate systems dealing with authentication process are PGP and X.509.

As it is been known the PGP trust model is used for authentication relating to electronic mail transactions type of applications between human beings. It supports a Web OfTrustmodel in that there is no centralized or hierarchical relationship between CA as it exists at X.509. The underlying hypothesis of the model are that a trust or may trust other entities, may valid date certificates from other entities or may trust third parties for legitimization certificates. An introduceris an entity that signs someone else's public key (and thus vouches for a name public key binding) (Lemuria Carter, Ronald Campbell, The impact of trust and Relative advantage on Internet Voting Diffusion, 2011).

A met introducer can sign keys as well as specify who the primary introducer is.
Also, any entity can function as a certification authority. Every key that a user trusts or signs have to have a degree of trust associated inside to it, namely: categories such as unknown, untrusted, marginally trusted or completely trusted. It is also assumed that a user has an implicit trust (the highest form of trust in this model) in her/his own key. For example, a client can specify that she only completely trusts a key if it is marginally trusted by a meta introducer in our case the committee and completely trusted by a (trusted) introducer (machine).

Once keys are registered (along level of trust within) with the PGP system, then it computes a validity score (if an Ack has been established and is for the right person, balloter). It is now the responsibility of each entity to query the system and to acquire the keys by the server entity which is for authentication.

The X.509 another trust model but it's an hierarchical model for authentication. Each entity must have a certificate that is signed by the central CA or another authority, which has been directly or at second hand certified by it. This model assumes that certification authorities are organized into a universal "certification authority tree" (it's like a list) and that all certificates within a local community will be signed by a certification authority that can be fitted into this tree.

Due to PGP's lack of official mechanisms for the creation, acquisition and distribution of certificates it is considered unreliable for E-Commerce, but appropriate for personal communication. X.509's rigid hierarchical structure may lead to unnatural business alliances between competing companies that violate the natural order of trust. Some applications, such as the reference information distribution systems described in section 7, need certificates to have a lifespan longer than is currently allowed by either scheme(Lemuria Carter, Ronald Campbell, The impact of trust and Relative advantage on Internet Voting Diffusion, 2011).

4.7 Preview of trust issues about previous e-votingenvs

Since classical style voting was gradually replaced by electronic voting machines or even better Internet voting, this led to repercussions in various countries. In the USA, public pressure has enforced the printing of paper copies of each vote cast on a machine (Mercuri, R. (2002). A better ballot box?. IEEE Spectrum, 39(10), 26–50). In Netherlands, electronic voting has been abolished altogether based on the research and weigh on a pressure group. Parallel to these developments, new electronic voting schemes were designed in computing science, but the security of such schemes is complicated, and users may not be easily convinced. In the testing trajectory of a Dutch Internet voting system, too complex vote verification procedures reduced trust in the system.

4.7.1 Trust in e-voting (political elections)

Adopting an e-voting system means that maybe there will be an increase voter turnout and reduction at residual (uncounted) votes. Regarding the effect of the electronic

system on voter turnout and residual votes, empirical evidence turns out to be mixed so far. Some scientists, in particular (Ansolabehere and Stewart (2005)) suggest that existing voting technologies differ significantly in their effect on residual votes. But, Card and Moretti (2007) analyze the effect of touch-screen voting for the 2000 and 2004 U.S. presidential elections, and they found negative effect on voter turnout. Regarding these mixed results, Allers and Kooreman (2009) suggest an analysis of different effects on national and municipal elections. This means that voter's intention has been effected by variation type of the elections. The distinction between presidential and local elections is in awe of big interest for many researchers.
E-voting systems have different effects on voter participation according to available studies, although few systematic analyses have been conducted in the United States. One empirical study reports that e-voting has a positive effect on turnout in municipal election but on the other hand it has a negative consequence in national elections (Allers&Kooreman, 2009).

But there is no guarantee that the latter argument is the only correct, so there are some other elements for voter's intention which including polling station density and social pressure. Voter's intention is connected to trust issue and applies to the system. This shows that it is necessary to empirically examine whether there exist different effects of e-voting on user intention to participate in presidential, gubernatorial, and local elections or European elections for the other regions.

4.7.2 Trust at stages of e-vote

In the voter registration process those searching for election trust the PA that only eligible voters are included in the formation of the electoral registration. In turn due to the process followed for voter registration in the UK (home occupant/s registration as opposed to personal registration), there is a considerable amount of trust from the PAs to the voters during this stage.

4.7.3 Trust flow during casting

When a voter casts a ballot, one trusts the PA to be provided with correct ballot paper, a private environment is maintained, to verify the secrecy of one's choice, and safeguard the ballot itself until it has been counted. In the case of e-voting system each of these four reasons generating voter trust towards the PA is accordingly affected. PAs have no standard of securing that voters will be presented with correct

ballot paper other than trusting that e-voting system performance will be maintained by the suppliers according to the promised standards. The same thing should be applied in the matter of keeping the voters' e-vote secret. Although voter data and cast ballot data are stored separately to maintain voter anonymity, in the UK for example there is a legal requirement that ballot can be back traced (trace route) to voters ID for judicial verification of the election process.

Furthermore, the technical means are available to allow such a process to happen.Mercuri and Neumann referred to the matter of personnel integrity in relation to the Security of e-voting processes, a breach of which could lead to the disclosure of e-vote content. Similarly the PA has no means to safeguard the e-ballots cast until they are counted. E-votes are stored within the e-voting systems and yet again PAs have to trust system suppliers. In privacy point of view the trust flow is inverted. While in traditional voting PAs have to provide voters with a private environment to cast a ballot, in remote internet voting unsupervised voting it is PAs that have to trust voters to cast their e-ballot in privacy. As voters are in possession of their remote voting credentials, they have on their hands control of the level of privacy that they require to cast a ballot providing that they own the technical means to do so. Pa's therefore trust that each individual voter will make legal use of one's voting credentials and will not use votingcredentials maliciously (i.e. the credentials of the previous occupier of a house, or incorrectly delivered credentials) even with their consent (i.e. family member voting).

4.8 CIA

Confidentiality Threats

The basic concept of the prevention confidentiality to a system is Unlink ability between ballot and voters ID.

It is important to protect an electronic voting:

- Eavesdropping
- Wiretapping
- Misdelivery
- Exposure of personal data to the network

Most specific vulnerabilities for the upper principle are:

Hardware and Software

- Modification
- Substitution
- Lawful interception

Software scope:

- Software deletion
- modification
- Trapdoor
- Easter egg
- Logic bomb
- Information Leakage
- Virus

Integrity threats:

When you speak for integrity you mean system accuracy, consistency. Safeguarding process must guarantee that votes cannot modified, forged or deleted without detection. At this principle reliability is fundamental which means that the election system should be robust, without loss of any vote and be trustworthy to the people who are participate in.

Additionally integrity refers also at personnel and data. Although, integrity has to protect the system from:

- Wiretapping
- Masquerade attack
- Falsifying or malformed messages
- Web interface spoofing
- DNS attack
- Malicious code or dll on clients machine

The vulnerabilities are the same as for the confidentiality.

Authenticity

More analytical, it means that transactions and communications are genuine .The voting countering must protected from reading from external during the voting process.

Authenticity means that the system is protected from:

- Impersonation
- Random guessing
- Eavesdropping
- Spoofing
- Session hijacking remotely
- Man in the middle

4.8.1 The security mindset

Ideal e-voting systems must include privacies of individual voters, must be able to convince people that the voting is accurate and democratic, must disable any entity to coerce voters to choose a candidate it is supporting, and additionally must be able to resolve disputes between voters and election administrators. Also, they must be robust against various intentional or accidental troubles, must be applicable to large-scaleelections, and must be supported by practical assumptions. However, some of these requirements completely contradict each other, e.g. individual votes must be linked to their voters to convince people that all votes are legitimate, but these links reveal personal details of the voters, also they enable an entity to coerce voters to choose its supporting candidate more reliably. To protect a voter from being coerced by other entities, any link between a voter and its vote must be concealed even from the voter itself.

5 Chapter functioning & non functioning

5.1 Security & Technical Requirements

5.1.1 Requirements for e-voting system in depth

- The remote electronic voting system must has an appropriate identification and authentication system for the voter before he/she stores the vote in the ballot box.
- Specific control: *The* system *it must have the appropriate user identification process with which identifies and gives authentication at users using different kinds of authentication*.
- *Also the IS should identify and have authentication process for the devices, before opening connectivity!!*
- *The responsible corporation have monitoring tools, authorizes and inspects the remote access in all ways destined to information system.*
- *There will be a strong and restrict policy for access to privileges functions by firmware and processes.*
- The storing e-votes in the ballot box must be come from only the eligible voters so any other access to the e-ballot box shall be defined by the rules as dropped or denied.
- Specific control: *The* election *authority are developing and review a voter eligible list from which authentication permissions are coming from.*
- *The System itself when the client sign in to vote must have a policy which puts limitation on lo-gin attempts by the user during a time period. Also, usually is evitable to lock the account after failed attempts by the user.*
- One requirement that must have a specific control is non-repudiation which gives the system opportunity to identify when a specific client has taken

particular action. Additionally, timestamps and digital signatures should be employed on top of e-vote.

- At the remote electronic voting system shall be a policy to ensure the data protection law with respect to personal data before transmit ion process
- Specific control: *In this requirement what is needed is strong cryptography to protect the data confidentiality and integrity which has moral issues with trust by the clients*.
- Another 'principle' is that the remote voting system must ensure the confidentiality of the transmitted authentication information.
- Specific control: *The corporation must ensure that the communications are protected with applied cryptographic schemes that ensure data protection .This prevents from a man in the middle attack.*
- During the polling stage the e-vote system shall ensure the confidentiality of the transmitted e-ballots .Additionally, the remote electronic system must ensure that the protocol messages cannot be deleted without checking the content and undetected.

Specific control: *Usually, at this point the system itself must have checkups which protect the unauthorized change at software. There is also integrity check validation about errors, tampering information and other. The implementation of such verification automated tools should be centrally managed*.

Another control for the protection of CIA could be the collection of events that affect CIA and monitoring them. Also, audit information that come from audit process should be protected first of all because of confidential personal information so trust issue between client and the system.

- Also, in the remote e-vote system shall verify the authenticity, integrity, format correction of all messages before be in the action of process them.
- Specific control: *The e-voting system IS must ensure the authenticity, correctness, soundness*

- *Non repudiation should be implemented with usage of digital signatures and timestamps which tend to be helpful for validity & integrity of messages*.
- *Another one could be the creation of special mechanism that protects the communication session of the client!*
- The remote electronic system shall delete any kind of history related to voters voting from the voting casting machine when finishing the voting process.
- *The system itself must have the intelligence to provide the client with clean desktop after the voting at device with wiped clean process*. (Integrity policy).
- At the remote electronic voting must be not any provision of any information from protocol messages that links to what the voter casts.
- Specific control: *An* encryption *mechanism which provides protection at communication integrity and confidentiality!*
- There shall be also a policy to ensure that neither the ballot itself nor the number of choosing voting options nor a spoilt vote (length of the protocol message) can link to a particular voter. The sequence numbers from the messages shall not reveal something about voter's identity!
- Specific control : *In this part there should be according to NI-ST an encryption scheme at election process, which allows the voter to protect his privacy (homomorphic encryption, digital signatures)*..

5.2 Tallying stage requirements

The voting server shall protect the integrity & authenticity of e-votes when the polling stage has been finished.

- The software itself shall protect the integrity and authenticity of the ballots.

- Specific Control: *The* software *must have protection mechanism against unauthorized changes to software kernel etc. For example dll injection could be an attack!*
- Election data shall be protected by tallying software mechanism.
- Also, tallying software must ensure that its functionalities, operations and processes have not affected by other remote malicious activities or applications!
- Specific Control: *Partitioning the user functionality from IS management process.*

5.2.1 Operational Policies for electronic voting (remotely)

The voter should not has to lose his right to vote without actually vote.

If this doesn't committed maybe trust to the system and confidence would be affected in a bad manner

- Remote e-voting shall prevent voter interaction in case we have a malfunction.
- The Web interface must provide a confirmation code to the voter not the status of his vote but confirmation that the ballot has been stored correctly.
- The remote e-voting shall give a warning message to poll-takers if it has failures or malfunctions but at the same time should inform the client at the time of the voting stage that something wrong is going on so the confidence at the system be stable.
- Another point which is related to data loss is that protection policy for operations and in case of breakdown shall take appropriate action for prevent data loss (back up)

- The Interface for electronic voting in which the voter lo-gin should be enabled at all the polling stages!!

- Normally, the system itself should have robustness against physical attacks or power outage at the voting server, unexpected user behavior, env effects and network connectivity.
- The e-voting remote system should ensure that in case of malfunctioning, breakdown no voter loses his right to cast nor get the right to vote twice.
- Continuity plan should be enabled from the start because operations for the election process are crucial (ZisisDimitrios ,Methodologies and technologies for designing secure electronic voting information ,University of Aegean,2011)

5.3 Accuracy

When we say the system is accurate that means it is not possible for a vote to be altered. Secondary, it is not possible for a validated vote to be eliminated from the final tally. Also, there is no possibility for an invalid vote to be countedin the final tally. Accuracy is one of the most important factors to any system. If the input is not fit right, then the result will not be acure.

Not only should the system be accurate in counting votes and maintaining the integrity of cast ballots but the system must be accurate in identifying balloters.

Ballot secrecy

Usually in this part we have a weak hypothesis which states that the election system must ensure that vote of each voter cannot be find out about balloter vote. A stronger hypothesis is that don't affect the election process and nothing can be revealed in external or internal parties specifically manner of voting…

If your vote could be revealed that would make easier for people to buy your ballot and "sell it".

5.4 Voter Authentication

With this requirement as it seems, only authorized voters should be able to vote and also to vote only once a time or whatever the maximum limited number of times is. "A system is verifiable if anyone can independently verify that all votes have been counted correctly" (Cranor L. and Cytron R., "Design and Implementation of a Security-Conscious Electronic Polling System," *Technical Report*, Washington University Computer Science, 1996).

At Latest, many experts believe that the best scientific method to verify votes and perform recounting process is with paper ballots. In addition, the voter should be able to verify that his/her ballot is entered correctly and allow them to adjust their vote if necessary. The process needs to verify the validity of the voter as well. Maybe a solution to the upper is the use of a nationwide database of registered voters' information (where confidential data exists) and a method of non-intrusive biometrics could identify participants. This kind of system is being analyzed above.

Finger printing recognition, the electronic methods of recording and recognizing an individual finger print, advanced substantially during the last decade of the 21th century. Today, identification can be achieved in a few seconds with reasonable accuracy. As a result, the use of automated fingerprint identification systems (AF-IS) that record, store, search, match and identify finger prints is rapidly expanding. AF-IS can be integrated with a micro-controller and other peripherals to form an embedded system which is a comprehensive electronic voting machine with fingerprint print identification system (http://www.engineersgarage.com/contribution/biometric-voting-machine).

The system has to verify that the E-voting system has not been compromised at all. A voting system that performs both functions—voter identification and the casting of the ballot—is inherently open to strong criticism and potentially to malfunctioning. Even when the two functions are kept rigidly separate, there might be a possibility for inside operators to cross-check the two data sets. This possibility requires the

establishment of specific technical and procedural security measures to guarantee that these two sets of information cannot be linked under any circumstances. The secrecy of the vote relies on these measures and it is important that they can be clearly communicated and demonstrated to interested stakeholders International IDEA, *Electoral Management Design: The International IDEA Handbook* (Stockholm: International IDEA, 2006).

5.4.1 Privacy

Privacy is one of the most important attributes of an information system which has to be satisfied, in which systems the need to share information among different kind of entities, not trusted in most cases. A system is called private if neither election authorities nor anyone else can find link ability any ballot to the voter who cast it and no ballot-er can prove that he or she voted in a particular way (Cranor L. and Cytron R., "Design and Implementation of aSecurity-Conscious Electronic Polling System," *Technical Report,* Washington University Computer Science, 1996). Privacy is a wide spread concern to all users of a voting system. Since it is important to have an audit trail available to verify the system trace route, aggregation of data should be accessible as opposed to an individual's vote. Some voters have problems when they start using the voting machines which requires that a staff volunteer assists them and this can interfere with the privacy of the voter (Insider attack). The goal of the e-voting system is to search for a way to have simultaneously privacy as much verifiability in the system.

5.4.2 Reliability

A system is said reliable if it performs and maintains its functions in continuous manner. Reliability in the system calls for that there will be alternative methods if a failure occurs. For example, in the event of unavailability, the system should have an alternate power source or an alternative paper method. Many polls did not open on time because of machines malfunctioning (Donald Moniyan, Building secure elections, Texas A&M University, 2004).

5.4.3 Verifiability

To ensure trust to e-voting counting process the only thing that can be done is to verify into the system that a ballot of the voter was counted correctly.

There are two different kinds of verifiability:

First, universal verifiability, meaning that anyone who takes a role at the election process (voter, election authority) can verify the election outcome after the tallying process. To use universal verifiability you can adapt mix network mechanism.

Secondary, there is known as individual verifiability which means that every eligible ballot-er can verify on his own that his/her vote was counted.

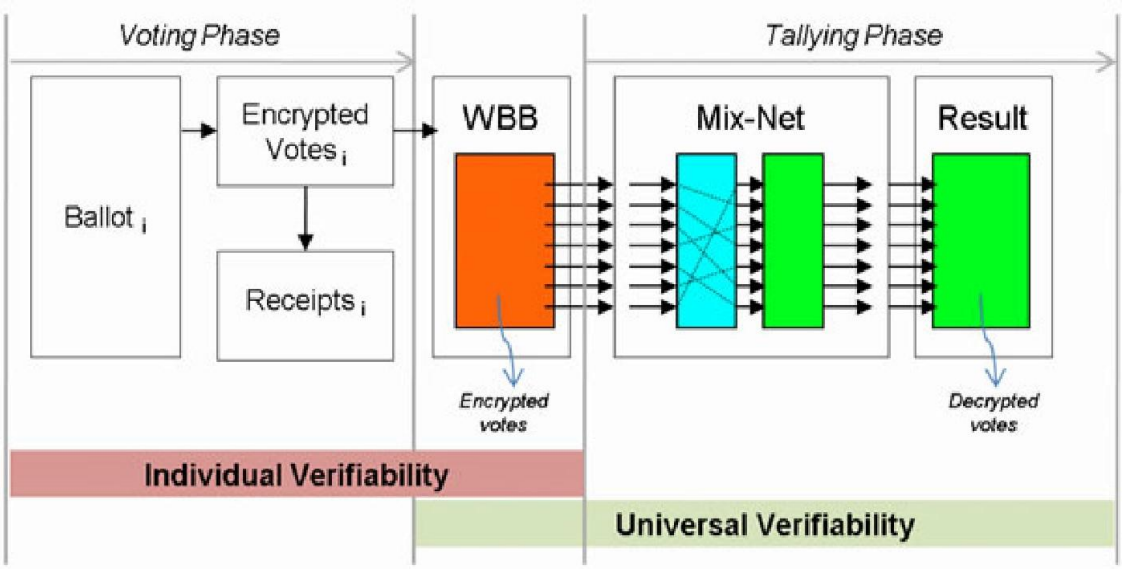


Figure 8 Verifiability

* Kremer inferred and identified another type of verifiability known as eligibility verifiability: It means anyone can verify that each vote in the published set of "all" votes was cast by an eligible voter, and anyone can verify that each eligible voter cast at most one vote.

5.4.4 Usableness

A system is convenient if it allows voters to cast their votes rapidly, in one session, and with minimal hardware or software equipment or needing special skills. The innovation of touch screens and integration into the voting process was first used

to aid the disabled population (those who are blind etc) . This increased convenience of touch screens could lead to higher voter participation and reduced time at the polls. If the system infrastructure utilizes technology that society is already comfortable using (is already trained at some point), voters will consider the system to be more convenient and will have confidence on it.

5.4.5 Mobility

Mobility in the system could allow voters the capability of voting wherever Internet access is available. This feature is better suited for an online E-voting system. Moreover, the designs of the physical machines need to be small enough to accommodate many polling locations where space could be an issue (http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0005/16097/Implementationofe-votingsummary_6720-6268__E__N__S__W__.pdf).

5.4.6 Flexibility

The system is considered to be flexible if it allows a variety of ballot question formats, including open ended questions. Flexibility is needed for write-in candidates and some survey questions. Nevertheless, the system should be dynamic especially in our fast-paced society. Additionally, the system should be able to accept more than one method of inputs to accommodate both voters at the polls and absentee ballots (http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0005/16097/Implementationofe-votingsummary_6720-6268__E__N__S__W__.pdf).

5.4.7 Receipt-Free

Some voters claim that election authorities are dishonest or on the other side election authorities detect dishonest voters, disputes between the authorities and voters about liability for the dishonesties must be resolved without disclose of any privacy of honest voters. The important thing is that the election authorities cannot reveal any of their secrets. For example, when the authorities reveal their encryption or decryption

keys, votes of other honest voters also may be disclosed. This ‘requirement’ prevents vote buying and coercion. Before the election process someone maybe he can urge or manipulate a voter to cast in a particular way (bribe or coercion).The attacker can make the voter how the behavior of himself should be during the e-voting process (for example generates for random bits).During the election stage the attacker can monitorthe traffic between the voter and the election authorities. If the election process has terminated attacker searches for proof that the voter casted in a particular way but on the other hand if the e-voting system has policy which protect privacy, the coercer cannot detect what the voter casts or open the e-ballot itself. With an in-coercible requirement adopt at e-voting scheme the voter has the privilege to change the secret information of his ballot and open his/her ballot in a desired way so the voter can provide the coercer with false proof.

5.4.8 Democracy

A system has to include democratic issues it permits only eligible voters to vote and in second hand it ensures that each eligible voter can vote only once a time. . This characteristic can be accomplished by merging accuracy and verifiability. At last years, many counties require that voters vote in their own compound so, that everyone can assign himself in the approved voter list. In other cases some counties have implemented a database that tracks voters. A ballot-er must be able to show proof of his/her identify, the database is then updated, which prevents that voter from going to another vicious circle.

5.5 Social Admission

A system has social admittance if it has favorable reception and is considered by the public as being an effective system. It can be easy to inspect the users involved in a system. Even if the system is sound, users are what make or break the system. Perception is crucial. Last years, society views the majority of E-voting as inaccurate, unnecessary, and not private (Parakh A. and Kak S., "How to Improve Security in Electronic Voting," *Ubiquity Information Everywhere,* vol. 8, no. 6, pp. 1-7, 2007).

5.5.1 Robustness

If an attack has been faced at a fixed elections time there is no provision in the law of many places to postpone the Election Day if the voting machines are not working properly.

This requirement guarantees that there may occur a temporary collaboration either voters or authorities (legal malicious) which could disrupt the electoral process.

This situation includes the possibility of abstaining voters without the occurrence of problems as well, too, and to prevent unlawful acts which may void the outcome of the election. The requirement of resistance (robustness) also concerns that the security of the system must be satisfied in relation to external threats and attacks etc. denial of service attacks (DoS attacks).

5.6 Other requirements

Cost effectiveness: Maybe there will be no unlimited resources to spend on the voting system.

Accessibility: All categories of voters can vote, who are physically disabled or blind, nearsighted or illiterate can participated in the election process. In this attribute e-ballot system has given at voters can be included trust relation to the system because if a group of people who couldn't cast a ballot at past are going to participate in the future so increasing confidence ,trust can be a controller to the upper .

Equal accessibility, as a precondition of democratic issue, means that the e-voting system to be introduced should not be a complicated mechanism, i.e. it must not be "a test of computer literacy". From the voters' point of view, the system should be easy to use and should require no pro skills.

On the contrary, it should be user-friendly (has G.U.I) and independent of the voter's education, age, and physical condition. As a result, an e-voting system should be developed in such a way as to facilitate its usability and to preserveits controllability. But this require additional education, as well as organizational measures (help desks, e-election officials, etc.), to be effectively resolved (An Internet based electronic voting system, Legal and regulatory issues on e-voting and data protection in Europe, EU-IST-2000-29518 (D. 3.4.)).

Intelligibility: If the voters cannot understand how the count can be produced or why to accept the results coming from the specific system that would be a failure. It's a basic value for our society.

6 Chapter Discussion & conclusion

6.1 Proposed solution how to increase trust

The significance anonymous credential systems (or system of pseudonyms) was imported first time from Chaum in 1985. The entities that participate in anonymous credential system they are the users and ganismoi. The organisms undertake the publication and verification credentials while the users safeguard their anonymity.

The two basic requirements from such a system are, from the side of the organism that publishes and checks credential safety and from the side of user the aid of privacy protection.

When we say safety we mean that credentials are protected from escape, scripture and malicious attacks and only their real holder are in position it proves their possession. This means that credentials they cannot be used from somebody that does not belong to him neither divide because it does not become but because it is disadvantageous in the user. Simultaneously the users should remain anonymous. This is translated for the organisms that they do not possess other information for the user beyond that it possesses certain concrete certificates and also with regard to each it's credentials and pseudonyms they cannot be connected (linked).

Concisely, at the operation the user is supplied by the editor (pch European institution) a credential that contains all information which the editor is in position he certifies for this. When the user later needs he proves the validity of his elements in a provider of service he uses identity mixer for sure transformation credential. Credential afterwards the transformation it will only contain the subset of certified information which it wishes it publicizes. Beyond this the user can make transactions without these are connected from each other (unlink ability).

Description of IDEMIX solution

The technology idem-ix (Identity Mixer) was developed by IBM Research- Zurich with a view to it provides a powerful mechanism of anonymous identification and

protection of privacy (authentication & privacy) between users and benefits. In the operation of system involve dare users (users) and organisms (organizations).The organisms are persons in charge in order to they provide (issue) the credentials in users or they confirm (verify) if some user it possesses somebody concretely credentials. The term verifiers that will be used corresponds in these organisms. Be marked that a organism in the same transaction can be issuer and verifier as an example when he is required credential that requires possession of other credential.

Idem ix credentials are published from the issuing authority who certifies validity of certain characteristics of users as date of birth, rights of access etc. The main protocols that are execute dare the credential issuance and show proof protocol which use Camenisch-Lysyanskaya signature scheme. Essential condition for the correct implementation of protocols is the use of same parameters of system (group parameters, system parameters). When is executed to issuance protocol or certificated/issuing authority (CA) creates/publishes a credential for user with base his choise. The credential is signed by the CA with hers issuer private key and thus it can easily be verified with issuer public key. The credential also contains the pseudonym of user, which cedes the master secret user in credential.

Contrary to other technologies that dispatch certificates ceded in some pseudonym in the verifier (for verification), the systems that are based in idem-ix they only dispatch proofs (“I am bigger than18¬, “I am student¬). When the user demonstrates the credential in certain other entity (other user or service provider), substantially it does not demonstrate himself credential. In order to “pursue another entity the user that it possesses signed proof that his characteristics fill the determined conditions, they are executed zero knowledgeproofs.

The proof of null knowledge (zero knowledge proof) here means that this characteristics that are revealed were certified from issuer. The use of zero knowledge proofs allows in the user to demonstrate same credential continuously without put it in danger to connect the energies/his information from certain other entity.

The user has the possibility of using some pseudonym in order to it acquires credential from somebody issuer (issuing organization) and later it shows him in another organism while it uses other pseudonym. Evenif all involved organisms collaborate they cannot connect a pseudonym with which it was verified the

credential with pseudonym with which it was initially published. Thus, credential it can be used above times in the same organism without needs each time the organism it knows that this are done from the same user.

With idem-ix it cannot be published the credential if application does not become to suitable issuer and also the imitation or counterfeiting is impossible. When it is published credential in some user then this is also committed in the particular pseudonym hence in the particular user, however the issuer or verifier does not know who is this user in reality. Credential that was committed in pseudonym of concrete user it is impossible to be used from other user. Somebody here could suspect that he is possible somebody it gives his pseudonyms and credential that possess in some other, but the system idem-ix attend this it is particularly disadvantageous after it amounts with we give in somebody access in all of us the accounts.

Summarizing, from the moment where the idem-ix it allows in user to participate in the process of revelation of his personal data, the system itself decides also who from them and if it reveals him. This allows in the users to make anonymous authentication, thus anti give the all elements of their identity, the users they can acquire access somewhere proving simply that they observe the minimal conditions of use, without even reveal how they observe him. The user reveals selectively the elements that are essential for credential without releasing irrelevant information (personal data additional). That's why this and anonymous credentials constituting basic component for the protection of privacy in the digital world.

Idem-ix it materializes the below principles:

- The user has complete control and comprehension of his energies because he participates in the transactions where they are used credential and in the same time consent for the use of his personal information.
- The pseudonyms and credentials are only demonstrated when it is necessary.
- Only essentially involved (issuer & client) they take part in a transaction in idem-ix.
- The pseudonym of user is unique for certain concrete cross correlation thus cannot be used elsewhere on the contrary the keys of organisms they are public keys (public keys) bidirectional operation.

6.3 Main Functions

In order to be achieved the two basic requirements of safety and privacy idem-ix it uses the following attributes:

- Unlink able pseudonimity after the users use pseudonyms for the communication with the organisms, the organisms is not in position they gather information on the identity of users from these pseudonyms. Consequently neither they can connect 2 different pseudonyms from each other, nor different uses of somebody's credential that correspond in concrete pseudonym. Simultaneously users cannot sway from each other pseudonyms because this amounts with revelation of their personal data.

With use of systems of signature an organism can provide credentials signing a combination that is constituted by the pseudonym and a price that it represents credential (value). In order to signs a credential organisms are only required the knowledge of pseudonym thus master key and the genuine identity of user remain unknown in the organism itself.

- Verification credential with use of proofs of null knowledge (Zero- knowledge verification credential). With use of combinations of proofs of null knowledge the user has the possibility of proving in some organism that it has in the possession somebody credential without reveals his true identity, nor the pseudonym with the editor.

Up until now, there are already trust models which infer about public key infrastructure systems in general. In particular, these models address issues about authentication mechanisms and processes between sender & receiver as actors, message integrity, data security & confidentiality.

All these issues that were addressed are all elements of a security model but there is often a contradiction between terms trust model & security model like they are siblings. From user aspect of view security in general plays a significant role in trust

especially at computer based technology which will perform the requested function from user intention. Furthermore, other factors except security are same significant as security is from user's point of view. Another important factor which is connected with users trust at technology is usability or a sub – component of this is simplicity for a computer based system. Some other additional factors could be reliability of the system is in use and availability.

6.4 TPM in E-voting

Meaning: The TPM is a microcontroller which is embedded on motherboard of computing device, which is capable of storing key, digital certificates and passwords.

TPM offers security for the data that are stored on personal computer of the client and also provides the right level of certified security.
TPM has an interesting attribute which is memory curtaining (the isolation of PC's memory). Memory curtaining which prevent programs such as (virus's) which may create an issue at PC's memory with TPM. TPM also aims to overcome the threats posed by screen grabbers (hacking programs). Remote attestation
Feature TPM detects any changes un authorize made to the E –Voting system software. In this solution there is Trusted Network Connect (TCN) which provides a framework for multi-vendor network standard like Authorization, Access Policy and Isolation which helps to boost the security for E- voting system network.

You can see the following figure where an architecture view can be seen:

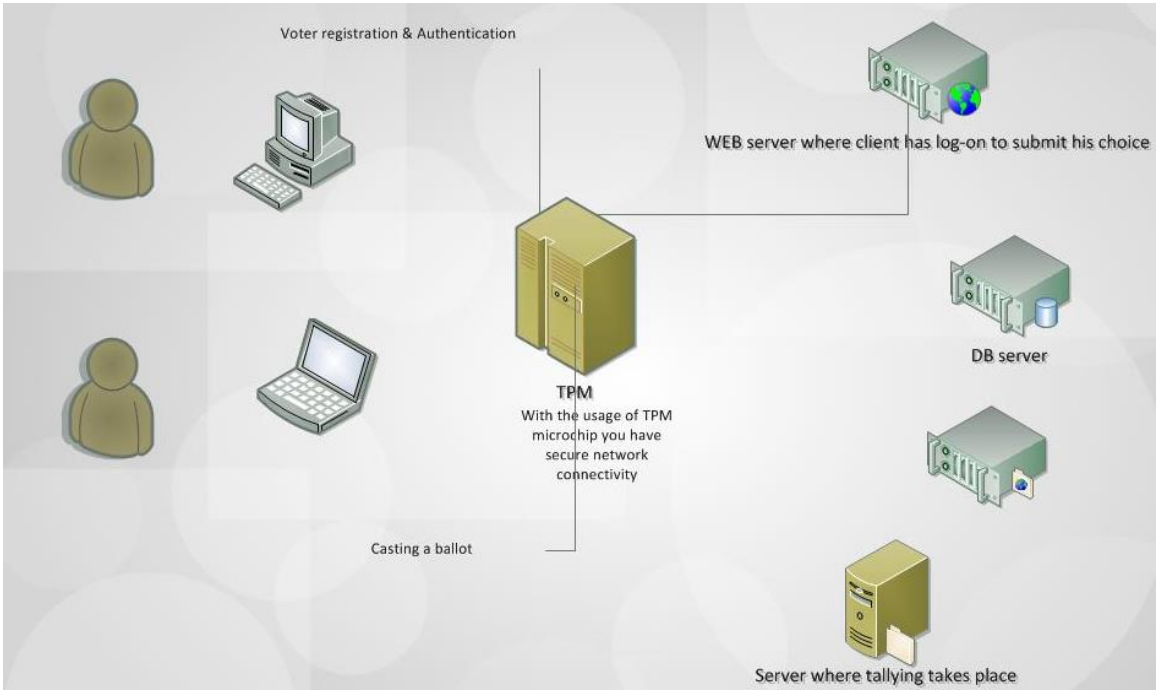


Figure 9 TPM Source: Ecpet, VTU INDIA et SEAIT VTU INDIA

A framework for trust in E-voting

A reliable model of trust must be conclusive and predict how usability, simplicity, availability & security principles affect user's trust in specific computer based technology system as electronic voting is.

In general, a trust model and some trust metrics can be introduced to measure user trust at specific computer based applications before the full development effort and installation process has been started.

The trust model that will be created must have a combination of security, availability, usability (simplicity), integrity of information, reliability & privacy for the user himself/herself. Until today, there are some security models in development that issue some aspects of measurement. Also, Trust model might have different kind of users some of which are officials, balloters or talliers. So maybe trust level will have different outcome to these different actors or entities.
Current trust models have been deployed based on security practices and issues only.
Some features that will be combined at the proposed trust model:

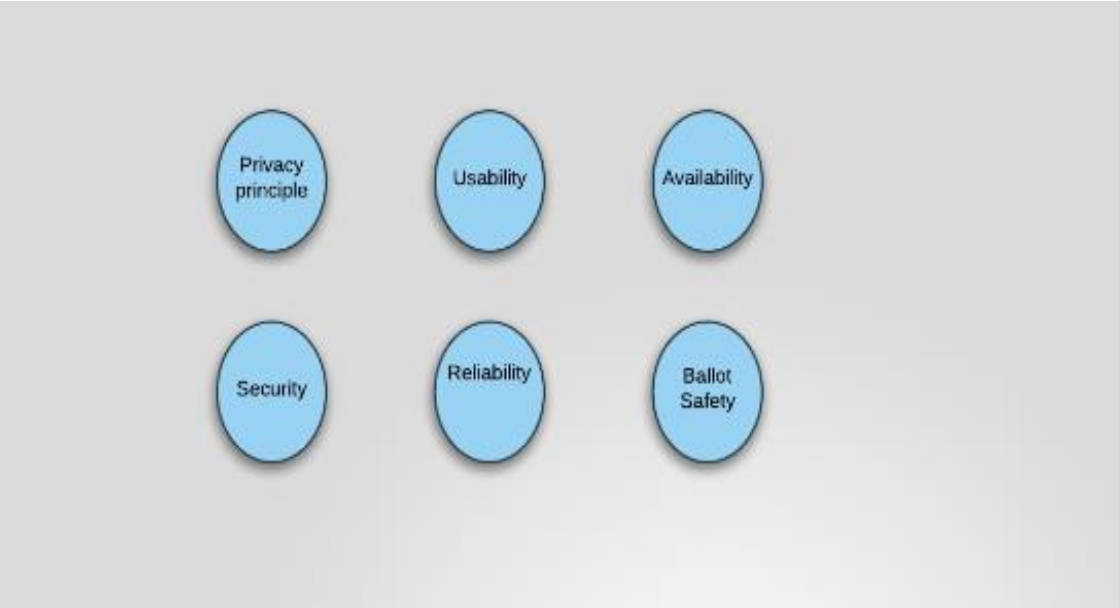


Figure 10 Components of combined

Problems Identification:

Problems with PKI architecture:

The usage of PKI has some cons such as

- Key exchange between sender & receiver. It doesn't meet specific principle which means that Verification mechanism of whom did send the 'r' message doesn't prove sender true identity until will be verified otherwise.

Other problems:

- Unauthorized access to network especially when you have Windows logon because authentication data are been stored in hard disk and information can be disclosed.
- Unauthorized access to platform with Biometrics that can be spoofed and because they are unique there will be a huge problem.

Security: Confidentiality and Integrity are applying to the electronic voting system except availability principle.

Another important thing is that the prior research has focused in psychological perspective of trust definition (Muir, B. Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems. Ergonomics 37 (1994), 1905–1922).

Metrics: Must exist to define measurement of user trust. Some aspects of the trust model (e.g., cryptographic techniques for enhanced system security or redundancy features to increase system reliability and availability) are generic and can be applied to more than **one** system.
Other aspects of the model may be specifically designed for a specific application system.
The proposed model also outlines the connection between verification and trust. Different examples of this connection can be analyzed, including blind trust, trust with verification, trust based on experience, and trust between principals and agents (more specific propagation of trust).

Because a computer based system doesn't work properly without encryption mechanism's implementation and support of cryptographic algorithms are important to the strength
Of the trust model, regardless of what specific application is been analyzed. In establishing trust in a transaction using a distributed computer system, users will ask some of the questions such as:

- Is this connection (transaction) being monitored by unauthorized parties?
- Are the integrity & data flow been protected from alteration?
- How can you prove your identity to the other party you connected to?
- Can you identify the true id of the other party (recognition) ??
- Can you admit that verification process & tallying are properly work?

Cryptographic mechanisms are existing for example anonymous signatures that helps the client to demonstrate possession of a credential for authentication while you have protection or maintaining the privacy of the user. Another, mechanism that boosts the

confidence is the usage of blind signatures which allow digital data to be authenticated without disclosure of ID of the user giving the signature. Receipts that helps authentication, anonymity, data integrity, confidentiality in the e-voting system. Mixing the ballots with the use of mix networks is another strong mechanism to help improving the robustness of the system and protect the ballot secrecy in some manner.

Voting issues have raised questions in many countries and more specific in U.S elections of 2000 and 2002 whether users have confidence in the integrity of voting process. The problems which are related to that were voter registration, casting and tallying phase so there was a need for innovation to troubleshoot these problems. At the first place was initiated to replace unreliable voting systems such as punched cad ballots with newer systems that employ more advanced technology for voting , which is optical scan & DRE machines. On the first hand, there was improvement in some areas such as usability and reduction of unidented under voting, but the security and public trust for the new DRE machines is being raised.

So the trust model that will be in developing phase might be used to facilitate the successful deployment of the new technology to be used be the public. The model might have something like subsystems which could be: Vote registration, vote casting, vote tallying.

Variables list that will be included at new model for electronic voting could be the following:

Πίνακας 1 Subsystems of model

Trust model subsystems	Parameters

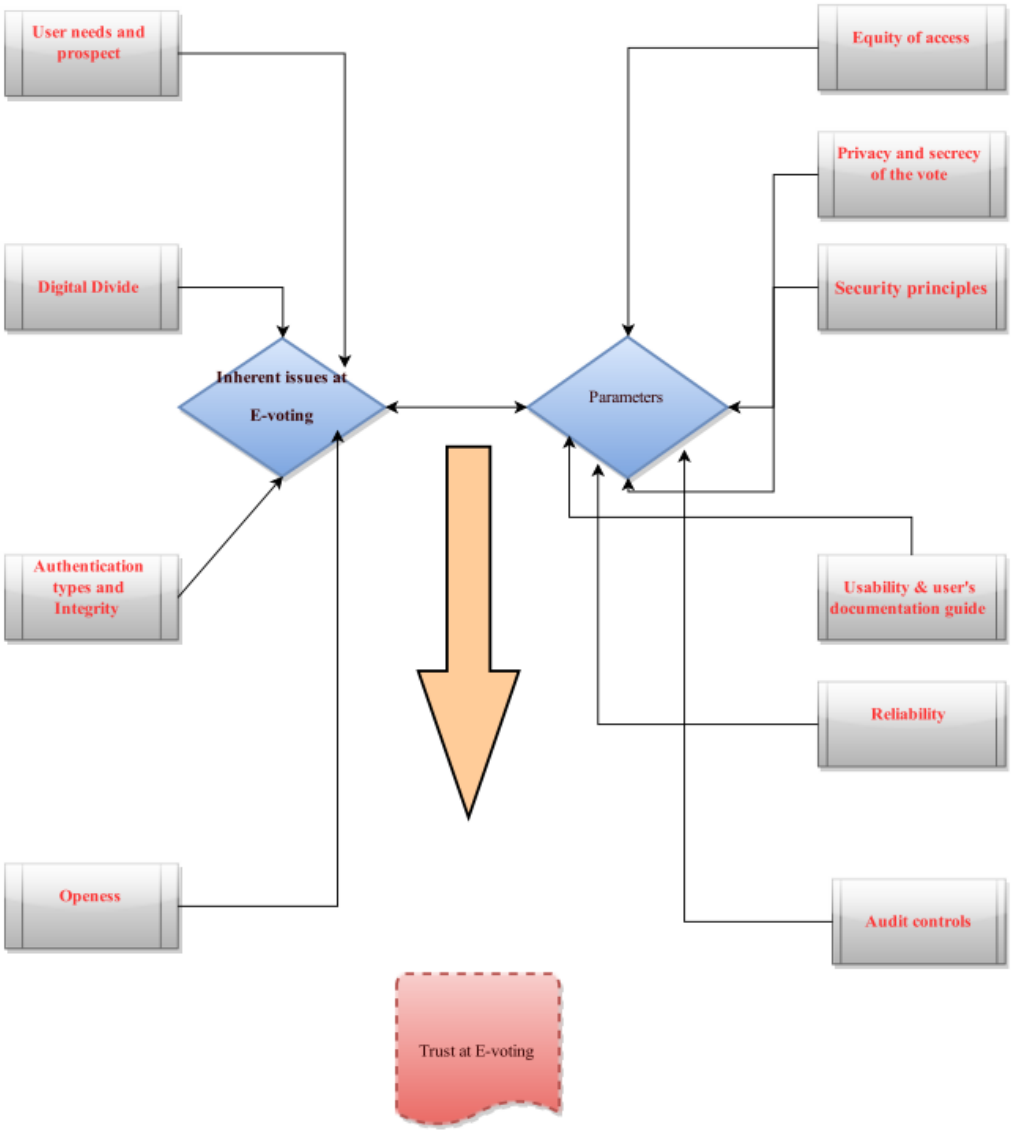
Security	Authentication mechanisms during the registration and vote cast process. Integrity of voter registration database, vote casting database. Verify voter's identity. Verification of ballot integrity.
Usability (Simplicity for the user)	Ballot structure design Remote electronic voting (How this will be work for user that are not have the required skills to use it). Documentation hardening about the simple user. Error preventing UI.
Privacy issues	Anonymity during voting. You cannot disclose the identity of the user from what he or she casted. Data confidentiality during casting. Ballot-privacy: No-one can outside of the system can determine what candidate has been checked from the user.
Reliability & Availability	Functions that are maintaining the system if a failure occurs. (Prevent malfunctioning) How robust is the system to denial of service. Quality of service to the public. Check if the quality meets the application e-voting criteria.

Table 2 Subsystems

Metrics for electronic voting systems might include:

- Voter confidence in accordance to the voter registration to cast a ballot to the system.
- The voter must having confidence that his vote will be counted at the end and the system will not reject his ballot.
- Existence of confidentiality at the vote!
- Only authorized users voted so balloter confidence might be affected by that.
- The anonymity requirement has to be implemented.

E-voting systems can be tested as a service to verify that the systems meet specific trust requirements of various groups of users (such as voters and election administration officials, bulletin board) and the systems will be iteratively refined until the systems meet acceptable trust thresholds. Furthermore, e-voting system users can participate in elections, and then they can provide input regarding their trust levels in these voting systems.


User needs and prospect
Digital Divide
Authentication types and Integrity
Openess
Inherent issues at E-voting
Parameters
Equity of access
Privacy and secrecy of the vote
Security principles
Usability & user's documentation guide
Reliability
Audit controls
Trust at E-voting

Conclusion

The truth is that there have been several studies in either hardware level either at the level of software to solve the trusting in e-voting issue. However none fully meets the requirements of confidence at such a system. Creating an algorithm could be a solution but in near future will eventually "broken." Perhaps the interlocking measures and perhaps it that some solutions give a satisfactory model that will solve this problem. And to solve this will bring radical changes and more nuanced in this field.

Βιβλιογραφία

Έντυπη

- Sang OK Ch oi & Kim, Journal of Information Technology, 2012
- IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf,policy paper, 2011
- Tadayoshi Kohno, Analysis of electronic voting system, 2004
- J.Nagler&M.Alvarez , A natural experiment of race-based & issue voting, University of Utah, 2001.
- Lemuria Carter & Fr. Belanger , The utilization of E-government services, Information systems journal, 2005.
- Allers, M. A., &Kooreman, P., More evidence of the effects of voting technology on election outcomes,*Public Choice*, *139*, 159–170, 2009
- Adida B Helios: Web based open audit voting. In: Fourteenth USENIX security symposium (USENIX Security, July 2008).
- K.MacNamara & I.Iedemska, A survey of Electronic Voting schemes, 2012
- R.Aditya ,Colin Boyd & Ed Dawson , Implementation issues in secure E-voting schemes, Queensland University of technology, 2004Evans M. and Fumell S.,"Internet-Based Security Incidents and the Potential for False Alarms," *Electronic Networking Applicationsand Policy*, vol. 10, no. 3, pp. 238-245, 2000
- Mayer, R.C., Davis, J.H., Schoorman, F.D.,An Integrative Model of Organizational Trust. Academy of Management Review 20(3), 709–734 (1995).
- Schlienger, T., Teufel, S., Information Security Culture: The socio-cultural dimension in information security management, Ghonaimy, A., El-Hadidi, M.T., Aslan, H.K. , Proceedings of the IFIP TC11 International Conference on Information Security, pp. 191– 202. Kluwer (2002).
- A.Antoniou, C.Korakas,...,A trust centered Approach for building e-voting systems, 2007.
- Luhmann, Niklas (2000) 'Familiarity, Confidence, Trust: Problems and Alternatives', in Gambetta, Diego (ed.) Trust: Making and Breaking

Cooperative Relations, Department of Sociology, University of Oxford, chapter 6, pp. 94-107.

- McGaley, M. and Gibson, J.P., 'Electronic Voting: A Safety Critical System', National University of Ireland, Maynooth, 2003.
- Lemuria Carter, Ronald Campbell, The impact of trust and Relative advantage on Internet Voting Diffusion, 2011.
- Mercuri, R. , A better ballot box?., IEEE Spectrum, 39(10), 26–50, 2002.
- Cranor L. and Cytron R., "Design and Implementation of a Security-Conscious Electronic Polling System," Technical Report, Washington University Computer Science, 1996.
- J.Nagler&M.Alvarez , A natural experiment of race-based & issue voting, University of Utah, 2001

Διαδικτυακη

- "E- Voting", Competence Center for Electronic Voting and Participation, Διαθεσιμο στο http://www.e-voting.cc/en/it-elections/definitions/ (last access 13/5/2015)
- C. Lambrinoudakis *, V. Tsoumas, M. Karyda, D. Gritzalis, S. Katsikas, The Impact of The Impact of 'System Actors System Actors to the Overall Security Level to the Overall Security Level, Διαθεσιμο στο http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/aegean/paper6.pdf (last access 13/5/2015)
- Electronic Voting Machines and Related Voting Technology, Historical Timeline, 2013, Διαθεσιμο στο http://votingmachines.procon.org/view.timeline.php?timelineID=000021#1975 (last access 13/5/2015)
- Biometric voting machine, Διαθεσιμο στο http://www.engineersgarage.com/contribution/biometric-voting-machine (last access 13/5/2015)