Modelling Threats of a Voting Method

Sven Heiberg Jan Willemson

Abstract

In Estonian Parliamentary elections held in 2011, the percentage of Internet voters among all the voters was as high as 24.3%. At the same time a student implemented a proof-of-concept malware which demonstrated the effective disenfranchisement of the voter from the right to vote. The paper gives an overview of risk assessment and threat modelling of Estonian Internet voting after the events of 2011. The paper presents a classification of attacks against the voting method, distinguishing between manipulation attacks, revocation attacks and attacks towards public confidence.

1 Introduction

Several countries have looked into some form of electronic voting for various reasons. It is hoped that remote electronic voting improves the availability of elections especially for citizens abroad and increases voter turnout [MM06, DSTW12, PC12]. Electronic tallying is seen as a way to speed up the process to provide accurate election results [MOP12]. For disabled people, electronic voting is a possibility to vote without assistance [LL07]. It is even claimed that without online voting segments of society will stay completely absent from voting[1].

Opponents of electronic voting point out that the application of new technology opens new ways to tamper with elections [JRSW04]. The basic threats are the same for all voting methods – selective voter disfranchisement, privacy violation, vote buying, etc., but the technology of electronic voting allegedly allows attacks to be carried out more efficiently than ever before.

Estonia has implemented a specific form of remote electronic voting – Internet voting – as a method to participate in various types of legally binding elections since 2005. In Parliamentary elections held in 2011, the percentage of Internet voters among all the voters was as high as 24.3%. In parallel to the rise of popularity, the amount of attempts to question the security or suitability of the Internet voting increased. For example, in 2011 a student implemented a proof-of-concept malware which demonstrated effective disenfranchisement of the voter from the right to vote, although the victim was left with an impression that his vote was cast as intended and accepted as cast. This proof-of-concept

[1] `https://www.bbc.com/news/technology-17846185`

malware was used as a tool in an attempt to revoke the results of Internet voting altogether [HLW11].

Today in Estonia, Internet voting is not a niche-method any more. Successful attacks against the method might have significant influence on the election result. In this evolved situation we have performed threat modelling of the Estonian Internet voting method. We have used attack-trees as a modelling tool. Building upon existing works and combining it with the experience from Estonian elections, we have reached an extended classification of attacks against the voting method. We distinguish between manipulation attacks, revocation attacks and attacks on public confidence. We show how the technology of the voting method can be abused to achieve an election specific goal.

2 Background

2.1 From Paper Voting to Internet Voting

By election we understand a formal process of selecting a person for public office by voting. Election depends on the voting methods available in the society to precisely gather preferences of those eligible to vote. The most widely applied voting method nowadays is voting on paper by secret ballot. Voting on paper usually takes place in the controlled environment of a polling station. A voter is authorised by the election officials; she receives a ballot paper and enters a polling booth, where she secretly marks her preferences on the ballot. The voter then inserts the ballot into a ballot-box guarded by election officials. The ballot-box is opened by the election officials after the voting period and the votes are tabulated by hand. All steps of the process, besides the actual act of voting, can be subject to monitoring by observers.

A remarkably different voting technology was applied in the United States before the American Revolution. Voters called their votes out loud, so that the clerk could write them down adjacent to the voters' names in the poll book [JRSW04]. Voice vote was an easily observable voting method, which allowed observers directly to verify the count, but the transparency of the method came with the price of bribery and coercion.

Voting by secret ballot hinders the coercion, provided that the act of voting is carried out privately and the cast vote contains no information to link it back to the original voter. On the other hand, ballot secrecy reduces the transparency of the tabulation and introduces new ways to manipulate the voting results by ballot box stuffing for example.

Harris observed and identified various types of voting fraud in the US elections [Har34]. He also analysed mechanical voting machines, already present at that time, and reached a conclusion, that "where election frauds prevail there should be no question about the advisability of adopting voting machines" [Har34, p. 280]. The new technology was seen as an effective countermeasure against fraud in the paper-based elections. Decades later the National Bureau of Standards (1988) strongly recommended the elimination of

the Votomatic-type of mechanical systems due to technological problems. The same report identified major vulnerabilities in electronic tallying systems. In 2000, a bad ballot design in the Votomatic system caused a scandal in the US Presidential election.

The advent of electronic voting methods took place in the 1960s with the electronic tabulation of paper-ballots. In the 1970s, electronics were used for vote recording by direct-recording electronic (DRE) voting machines. In 1990s, application specific electronic devices were slowly replaced by general purpose computers for voting [JS12].

By electronic voting we understand any voting method that relies on the help of electronic device(s) in performing any of its core functions – voter authorisation; voting; recording of the votes; storing votes for tally; tabulation of the voting result. By Internet voting we understand a remote electronic voting relying on the Internet as a communication channel between the voter and the electronic ballot-box.

The first legally binding Internet voting events were held in 2000 in Germany for the Student Parliament elections in Osnabrück, and in the United States for the Arizona Democratic primaries [Kri12]. Although experts acknowledged the need for new voting technology, the Internet voting in particular was accepted with scepticism: "Remote Internet voting poses serious security risks. It is much too easy for one individual to disrupt an entire election and commit large-scale fraud" [cal01].

In 2005, Internet voting was used in country-wide local government councils' elections in Estonia [MM06]. Since then, legally binding Internet voting has been applied by various other countries and organisations, e.g. Austrian Federation of Students [KET10], Switzerland [SGM+15], Netherlands [HJP05], Norway [GSB12], etc.

2.2 Analysing the Security of Internet Voting

The main source of uncertainty towards electronic voting is the human inability to observe and understand the electronic processes. A voter, using an electronic device on his behalf, has to trust the device to cast and accept the ballot as he intended. An observer, trying to judge whether the ballots are tallied as recorded, cannot tell the difference between a correct and tampered tally just by observing the device executing the tabulation software. It is impossible to determine whether the electronic voting device is correct with respect to the specification or the specification with respect to the problem. It is similarly difficult to determine that the software does not contain hidden functionality to perform a malicious function in addition to its public functionality. Even if we are well assured that the voting software itself is good, a malicious execution environment might change the behaviour of the software completely.

Internet voting, as remote electronic voting, adds additional layers of problems. Firstly, protocols used for Internet voting must be analysed with respect to attacks towards Internet communication such as eavesdropping, man-in-the-middle, denial-of-service, etc. Secondly, the Internet also serves as an attack

vector for installing malicious software to vulnerable systems exposed to the Internet. Attacks aimed towards voting systems are geographically unbounded. Even if the attacker is identified, it might be impossible to bring him to justice. If the attacker succeeds in taking over central components of the voting system the entire digital ballot-box is in danger. Thirdly, Internet voting, such as any remote voting method, must tackle the coercion attacks made easier by the voting from an uncontrolled environment. These problems call for systematic ways to assess the applicability of a given technology for the benefit of elections in a situation where there exists the will to commit fraud.

The response to the Arizona Internet voting pilot was the recommendation to delay Internet voting until suitable criteria for security are put in place [cal01]. Still, the development of the method continued and the project SERVE (Secure Electronic Registration and Voting Experiment) proposed architecture for an entirely electronic Internet voting system. A security analysis of SERVE stated that the Internet- and PC-technology have fundamental security problems which make it impossible to achieve an Internet voting system at least as secure as the current absentee voting systems. It was argued that even detected and neutralised attacks could have a devastating effect on public confidence in elections [JRSW04].

Barr *et al.* suggested, that election system standards should require vendors of voting systems to provide both threat and system models [BBD+05]. Shortly thereafter Jones stated that there is a need for a public catalogue of threats to evaluate the laws and administrative rules governing the conduct of elections [Jon05]. He built his voting system threat taxonomy upon the list of frauds by Harris [Har34]. Jones also noted that while certain threats target specific technologies, others are technologically neutral.

Buldas and Mägi made an attempt to compare the Estonian Internet voting to the system proposed by SERVE [BM07]. The authors used attack trees as an analysis tool. The comparison was made in several scenarios and the scenario of large scale vote buying was presented in detail. A report by the National Institute of Standards and Technology documented threats to remote voting systems applying postal mail, telephone, fax, electronic mail and Web server technologies for transmission of voter registration materials, blank ballots and cast ballots [Sal88].

In 2008, the US Election Assistance Commission initiated research on voting system risk assessment. In the first phase of this research, voting system models were created for seven voting technology types [TIR09]. In the second phase, a threat model was created for each technology type [TIR09, PYL10, PLY11]. Threats were identified at threat source – vulnerability pairs which were realised by threat actions combined into a threat tree which in the case of Internet voting consisted of roughly 100 nodes. Volkamer (2009) proposed a Common Criteria Protection Profile which defined a basic set of security requirements for online voting products.

Volkamer applied the profile to assess the Estonian Internet voting system, whereas most of the security objectives were met and none failed [Vol09]. Yasinsac and Pardue proposed a refined voting system risk assessment process based

on threat trees including voting system risk taxonomy and schema to facilitate the comparison and vali- dation of independent risk evaluations [YP11]. In their proposal, it was stressed that there are only two overarching voting system attack goals – either to alter or ensure a contest result or to negatively impact voter confidence. Unlike most other treatments they do not handle confidentiality as a root goal to attack the voting system.

Lazarus *et al.* aim to build a reusable and parametrised threat model for different kinds of elections which could be used for security evaluations in local jurisdictions [LDE11]. They only present five nodes of their attack tree, but the tree has been shared with and validated against research done by Pardue *et al.* [PYL10, PLY11].

Harris saw mechanical voting machines as a countermeasure to fraud [Har34]. Experts today tend to see complex technologies as a threat to democratic elections [cal01, JRSW04]. Electronic voting has some interesting attack vectors both for malicious insiders and outsiders. We combine this knowledge with experience from large scale Internet voting in Estonia to see whether there are any changes to the perceived threat.

3 Modelling threats of Estonian Internet voting

3.1 Threat Modelling Process

Risk assessment is a crucial step in the process of securing an organisation and its functions. By determining the likelihood of a given actor exercising a particular vulnerability in voting method and the resulting impact on the election, it is possible to decide which controls are necessary to mitigate risks to the acceptable level. Prior to actual risk assessment it is necessary to characterise the system and its threats. Although there are several attempts to use formal modelling to specify voting systems and analyse their security properties [KR05, RCE+06, WV11], we describe the processes, components, data and actors involved informally here.

We use the definition of elections and model of voting method to create a threat model which structurally defines the possible threats to the election and their materialisation through the voting method. The attack tree method lets us analyse the voting method from the viewpoint of an active adversary; it has been suggested and used for the analysis of voting systems by various research groups before us [BBD+05, BM07, YP11, PYL10, LDE11]. For the development of our model we built the basic structure on top of the tree presented by Pardue *et al.* [PYL10]. Secondly, we augmented it with the attacks we observed during the recent 2011 Parliamentary elections in Estonia documented by us both here and in [HLW11].

3.2 System Characterisation

3.2.1 Rules and Actors in the Election Process

By election we understand a formal process of selecting a person for a certain position by voting. The electoral process produces an electoral result, determining the composition of the office, is produced. The election as a process can be regarded as successful, if at the end we have a trustworthy election result, whereas the maximum amount of eligible voters has committed to this result.

There are 101 seats in the Estonian parliament and approximately 900.000 citizens eligible to vote. In the 2011 Parliamentary election, 789 candidates participated. It is evident that there is no such election result which will appeal to all. The distribution of the seats in the Parliament defines the parties that have a chance to implement their policy, and parties who have to form the opposition. It is important for both the winners and the losers that the election result achieved in the process is in accordance with the rules agreed upon by the society. The Constitution of the Republic of Estonia states the basic electoral principles. The Parliamentary Election Act defines Parliamentary elections in detail by regulating election activities such as candidate registration, voting procedures, etc. The Penal Code has defined several election-related criminal offences such as interference with election. From this data we extract ten basic rules for Estonian elections:

- **Authenticity:** only eligible voters are allowed to vote.
- **Freedom:** each voter can vote according to his/her free will.
- **Directness:** voter votes in person.
- **Generality:** there are opportunities for the entire adult citizenry to participate in voting.
- **Uniformity:** each voter has one and only one vote.
- **Ballot secrecy:** nobody besides the voter him-/herself knows how he/she voted.
- **Correctness:** election result is correctly calculated on the basis of cast votes.
- **Confidentiality:** election result is published only after the voting has ended.
- **Availability:** voting methods are available.

The violation of any of these rules might, given the circumstances, force the NEC to declare the election result invalid.

The Parliamentary Election Act defines the following actors in the election process: voter, candidate, and observer. There is also a hierarchy of electoral committees responsible for the election administration. The topmost committee

is the National Electoral Committee (NEC). The act and related regulations define for each actor the rights, role and duties for the role.

- **Voter:** Estonian citizen, who has attained 18 years of age by Election Day, has the right to vote. In Estonia the right to vote means, that a voter can give one vote for a single candidate. A voter must present an identity document to the electoral committee and sign the polling list against receipt of the ballot paper before voting.
- **Candidate:** Estonian citizen who has attained 21 years of age by the last day for the registration of candidates has the right to stand as a candidate. Any candidate has a chance of being elected to Parliament.

Both voters and candidates have a right to file a complaint against a resolution or act of any electoral committee, in case they find that the resolution or the act violated their rights. Any complaint filed against the NEC is handled by the Supreme Court of Estonia.

- **Observer:** The status of observer is regulated by the NEC. The person wishing to observe must apply for the status of observer, there are no clearly defined restrictions on the eligibility. Observers have a right to observe all election activities. Observers have a right to notify the electoral committee in case a violation of law is suspected. The electoral committee has a procedure to handle these notifications.
- **Electoral Committee:** There are three types of electoral committees – the National Electoral Committee, the county electoral committees and division committees. Those committees have a duty to organise elections on their level of competence. The function of the NEC is to verify voting results and election results across the whole country. The NEC has several other functions, it also has the right to invalidate the voting results on the polling division, electoral district, at county or the state level if some detected violation of the law significantly affected or may have significantly affected the voting results. In this case, repeat voting is held. If the Internet voting is cancelled before the actual Election Day, the electorate is notified and voters can revote. In this case, no repeat voting is held.

3.2.2 Voting Method

Elections depend on voting methods available in the society to precisely gather preferences of those eligible to vote and to produce a voting result according to these preferences. The voting method defines how these preferences are gathered. It is a technological, procedural and organisational structure to carry out the following core functions: voter authorisation; voting; recording of the votes; storing votes for tally; tabulation of the voting result. Voting results are inputs to the computation of the election result, therefore any problems with the voting directly affect the election result and confidence in the elections.

From the viewpoint of the threat model it is necessary to analyse the actors, procedures, technological components and data of the voting method, to see the possibilities to manipulate the voting result or the electoral principles.

There are two types of actors participating in the process directly – voters and electoral committees. The core functions are carried out in three stages – preparation, voting and tabulation. Voters are actively involved in the process of voting, whereas electoral committees are responsible for executing the process as a whole. It is possible for both voters and electoral committees to be corrupt. Although observers and candidates may not interfere with the voting directly, they have access to voting procedures which might give them access to the assets of the voting method. Both observers and candidates also have to be considered as possible threat sources due to their access and motivation.

We do not present the complete model of voting method here, but observe how the free will of a person eligible to vote impacts the election result through the act of voting. The first premise is that the electoral committee has included the person in the list of eligible voters in the preparation stage. It is also necessary that the voter is informed of the voting technology and procedures made available to him by electoral committee. During the voting stage the electoral committee authorises voters to vote on the basis of the voter's credentials. A voter uses a vote preparation tool to express his free will in the form of a vote, and the prepared vote is taken to the electoral committee by some means of transportation. The electoral committee accepts the prepared votes to a ballot box and maintains the list of voters who have cast their vote. The electoral committee stores the accepted votes in the ballot box throughout the voting stage. During the tabulation stage, the electoral committee opens the ballot box and uses a tabulation tool to determine the voting result according to the votes stored in the box.

We see that voting methods rely on several tools to perform their function correctly. These tools involve a vote preparation tool and the technical means for the transportation of a prepared vote for example. For the creation of the threat model, we need to consider cases where one or several of those tools are under an attacker's control. Additionally, the voting method depends on several types of data for its functioning. This data involves a list of eligible voters, votes in the ballot box and voting result for example. For the creation of the threat model, we need to analyse how confidentiality, integrity and availability of that data affect the voting result.

3.2.3 Estonian Internet Voting Method

Internet voting in Estonia is an instance of a voting method covering all the expected core functions. We give a short overview of the method, readers interested in more details are referred to Heiberg *et al.* [HLW11].

Traditional voting in Estonia is roughly divided into advance voting and Election Day voting. Internet voting is allowed only during the advance voting period and, unlike paper voting, is available 24 hours a day. Internet voting is made possible with smart card-based mandatory National Identity Cards (ID-

cards), which are used for identification and legally binding digital signatures in electronic communication. A voter with an ID-card and a computer can vote from anywhere. To counter the threat of coercion in an uncontrolled environment, the concept of revocation of an Internet vote (i-vote) is legislated. A voter can cast an i-vote several times, only the last one will be counted. An i-vote is also revoked if the voter uses any paper-based voting method during the advance voting period.

The Internet voting scheme consists of an i-voting application and an i-voting system. The i-voting application is an election specific application which allows the voter to cast their vote from their computer. The i-voting system consists of three servers responsible for i-vote collection, storage and tabulation. Only the server collecting the i-votes is exposed to the Internet. The digital ballot box is kept in the local network; the tabulation component is offline at all times.

I-voting system has a RSA key pair to protect ballot secrecy. The public key of the system is published with the i-voting application. The private key is stored in a tamper-resistant hardware security module used only by the tabulation component and protected by a multiparty authentication scheme.

I-voting takes place in five phases: setup, voting, revocation, tabulation and wipeout. In the setup phase, the i-voting system is prepared for election. The servers are set up with the list of voters and list of candidates. An empty digital ballot box is created and the key pair of i-voting system is generated in the hardware security module. The i-voting application is digitally signed by the National Electoral Committee (NEC); fingerprints and download location are published in newspapers and on the NEC Website. Steps in this phase are crucial for the integrity of the Internet voting result.

In the voting phase, the i-voting protocol is executed between the i-voting application and the i-voting system. The system verifies the eligibility of the voter and returns the candidate list corresponding to the voter's district. After the voter has selected a candidate, RSA encryption is used to produce an anonymous ballot. The anonymous ballot is signed with the voter's ID-card. The digitally signed encrypted ballot is sent to the i-voting system. The system verifies the signature and checks the status of the signing certificate by National PKI. If no problems occur, the i-vote is stored in the digital ballot box.

The voting phase is followed by the revocation phase during which i-votes of those who also have paper-voted are revoked. Revocation lists are prepared in polling stations and sent to the NEC. At the end of the revocation phase, the contents of the ballot box are anonymised – digital signatures are separated from encrypted votes so that the tabulation component will not be able to see which voter voted for which candidate. The anonymised ballots are transported to tabulation by offline means. For the tabulation itself, the private key of the i-voting system is activated and the anonymous ballots are decrypted.

If the term for filing complaints with the NEC and the Supreme Court of Estonia has expired or if final resolutions have been adopted in respect of filed complaints, the NEC registers the elected members of the Parliament. Thereafter all the media, which was used to handle and store i-votes, is destroyed physically. This is done in order to maintain the ballot secrecy even in the case

of breaking the encryption scheme in the future.

During all five phases, members of the electoral committee, responsible for carrying out election activities with the i-voting system, are observed by auditors and possibly voluntary observers. Central components of the system contain audit logs which makes it difficult to violate election integrity by controlling just one of the three servers.

The Estonian solution provides security against some problems with remote electronic voting. The revocation of an i-vote mitigates the problems with voting from an uncontrolled environment. It is hoped that a coerced voter has a chance and will to revote. It is hoped that the ID-card is too valuable for its owner to hand it over to someone else with their PIN-codes. Threats related to communicating over the Internet are handled by the mutually authenticated transport protocol used. Trust in the computers and vulnerability to the remote attacks from the Internet is a different story though. The security analysis of the system by Ansper *et al.* [ABO+03] claimed that in order to implement i-voting, it was necessary to find the compromise between the theoretical security of the voting scheme and the complexity of its implementation. Despite the need to trust central servers and computers of the voters, Ansper *et al.* found this compromise reasonable – an opinion which differed diametrically from the viewpoint of the SERVE report published a few months later [JRSW04].

3.3 Towards Threat Identification

3.3.1 Attack Tree

Attack tree like structural methods for security assessments have been used for several decades already. Called fault trees and applied to analyse general security critical systems in the early 1980-s [VGRH81], they were adjusted for information systems and called threat logic trees by Weiss in 1991 [Wei91]. In the late 1990s, the method was popularised by Schneier under the name attack trees [Sch99]. Since then, it has evolved in different directions and has been used to analyse the security of several practical applications, including PGP [Sch00], Border Gateway Protocol [CCF04], SCADA systems [BFM04], etc.

The basic idea of the attack tree approach is simple – the analysis begins by identifying one primary threat and continues by dividing the threat into sub attacks, either all or some of them being necessary to materialise the primary threat. The sub attacks can be divided further, until we reach the state where it does not make sense to divide the resulting attacks any more. These kinds of non-splittable attacks are called elementary attacks and the security analyst will have to evaluate them somehow. During the splitting process, a tree is formed having the primary threat in its root and elementary attacks in its leaves. Using the structure of the tree and the estimations of the leaves, it is then (hopefully) possible to give some estimations of the root node as well. In practice, it mostly turns out to be sufficient to consider only two kinds of splits in the internal nodes of the tree, giving rise to AND- and OR-nodes. As a result, an AND-OR-tree is obtained, forming the basis of the subsequent analysis.

3.3.2 Root Node for the Attack Tree

There is no general agreement among the researchers on what the primary threat should be for voting. For example, Lazarus *et al.* label the root node as "Change Result of Election Successfully" [LDE11], whereas Buldas and Mägi identify four different primary threats ("Large-scale votes theft," "Large-scale disfranchisement of votes," "Large-scale votes buying and selling" and "Large-scale privacy violation") [BM07].

Regenscheid and Hastings analyse threats to UOCAVA voting systems by assessing potential impact of a given threat to the security objectives of organisational operations, assets or individuals, those security objectives being confidentiality, integrity and availability, but do not attempt to form any kind of hierarchy among those threats [RH08].

Volkamer names six goals and motivations for attacker's intrusion in the case of remote electronic voting ("Compromising the secrecy of the vote," "Selling the vote / buying votes / force people to vote in a particular way," "Affecting the election result," "Computing intermediate results," "Confusing voters," "Collecting personal data") [Vol09].

Pardue *et al.* consider three primary threats ("Attack voting equipment," "Attack voting process" and "Insider threats") [PYL10]. In a later article, Yasinsac and Pardue reduce the number of primary threats to two ("Alter contest decision," "Undermine voter confidence") [YP11]. They also point out that the identified high-level threat must be tangible and measurable. For example, the threat: "Remove a ballot from a ballot box" is concrete, while "Change an election result" is inherently ambiguous [YP11].

A primary threat similar to "Alter contest decision" by Yasinsac and Pardue is brought out by all the authors. This primary threat is then developed into sub attacks which attempt to manipulate assets of the system in a stealthy manner. For example the root node "Change Result of Election Successfully" by Lazarus *et al.* [LDE11] is further divided into four attacks: "Attack Voting Equipment," "Poll worker Attack," "Perform Voter Impersonation Attack" and "Perform Vote By Mail Attack". All those attacks require disguising the effects of manipulation in order to be successful. The experience with Estonian Internet voting during the 2011 Parliamentary election shows that this requirement is too restrictive.

3.4 Parliamentary Election 2011

The first legally binding Internet voting in Estonia was held in 2005 during local government councils' elections. In 2007, the method was used for Parliamentary elections, where 5.5% of actual voters i-voted. In the 2011 Parliamentary election the respective percentage reached 24.3% totalling to 140 764 tabulated i-votes. The 2011 Parliamentary election differed from previous elections with the amount of i-voting related activity. In previous elections the issues with i-voting were mostly related with voters having some kind of technical problems with their computer such as missing ID-card software. In 2011, the security and

legitimacy of Internet voting was several times put in doubt.

Event 1: Student Attempts Revocation of Voting Result

Two days after the beginning of the Internet voting for the 2011 Parliamentary election, the NEC together with three major newspapers received an e-mail from student Paavo Pihelgas claiming that he had written a prototype of an election rigging malware. A version of this malware which selectively held back ballots for certain candidates was demonstrated to observers of OSCE/OHDIR and screened on National Television after the election had ended.

After the end of the Internet voting period, Pihelgas filed a complaint with the NEC demanding the revocation of all i-votes, reasoning that as the voter cannot check whether his vote was accepted by the i-voting system or not, the system did not comply with the Parliamentary Election Act. The complaint made it to Supreme Court of Estonia and was dismissed on the grounds that the person's right to vote was not violated, as Pihelgas knowingly put himself into the situation where he was disenfranchised by the malware[2].

Event 2: Candidate Attempts Revocation of Voting Result

Three voters turned to the i-voting help-desk with the following problem: the graphical user interface (GUI) of the i-voting application was too large to fit onto their computer screen and two candidates on the bottom of the list were hidden by the Windows task-bar. The problem was caused by fixing the minimal supported resolution for the GUI – a bad software design decision.

The Parliamentary Election Act declares that if there are any independent candidates in addition to party lists, they will be placed at the end of the list of candidates. This means that those hidden candidates were with high probability independent candidates. In the 2011 Parliamentary election, the confrontation between political parties and independent candidates was a major theme so the problems with displaying candidates were used as one example of discrimination of independent candidates. One of those candidates – Henn Põlluaas – filed a complaint to the Supreme Court of Estonia and demanded the nullification of i- voting results. The complaint was dismissed due to procedural problems[3]. The NEC had previously explained to the candidate that all 3 voters who encountered this problem received help from the election hotline.

Event 3: Invalid i-Vote is Found During the Tabulation

One of the i-votes was registered invalid by the tabulation component during the tabulation phase of the election. The Estonian electoral system does not consider invalid votes as part of the election result and the i-voting application has no functionality for casting a blank ballot. A voter who wants to intentionally

[2]Decision of Supreme Court in the case number 3-4-1-4-11. In Estonian. `https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-4-11`

[3]Decision of Supreme Court in the case number 3-4-1-6-11. In Estonian. `https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-6-11`

cast an invalid i-vote must either develop an i-voting application that makes it possible to encrypt random data, or find a way to manipulate the current application to cast an invalid vote.

The situation was analysed – errors in con- figuration were ruled out and no bugs were found during additional testing. The possibility of re-decryption of the invalid i-vote was considered shortly, but then abandoned – the encryption is the strongest measure to protect ballot secrecy in the system, therefore no ballots should be decrypted in isolation. If the isolated decryption of a single ballot were the case, malicious committee members could collude to break the ballot secrecy with help of the audit system. It was later understood that even if we knew the content of the invalid vote, it would be impossible to distinguish between a software bug and intentionally invalidated vote. There is currently no solid evidence about the actual events behind the invalid i-vote.[4]

Event 4: Elderly Woman Re-Votes 500+ Times

During the inspection of i-voting log files, an unexpected behaviour was detected by system administrators – an elderly woman had cast more than 500 i-votes over several days, peaking to 42 votes in an hour. The frequency analysis of the behaviour showed that, although suspicious, the pattern could be achieved by a human being. Although re-voting any number of times is legal, the woman was contacted, because it was suspected that somebody else was using her ID-card. She claimed that it was her who i-voted as this is perfectly legal and only the final i-vote counts. We have no other information to motivate her behaviour.

Event 5: Political Party Attempts Revocation of Election Result

Following the complaints by Paavo Pihelgas and Henn Põlluaas, one of the major political par- ties – the Central Party – also filed a complaint demanding the revocation of election results as a whole. The complaint was dismissed for similar reasons as the previous ones[5].

Event 6: Anti-i-Voting Movement

The Internet voting related activity went on for several months after the elections. A forum of the municipalities dedicated to i-voting was held. The Statement by the VI Municipalities Forum (2011) claimed that "both the statutes governing e-elections and the manner of conducting e-elections are in conflict with the Constitution." An anti-i-voting book about security risks related to

[4]Later, during 2015 Parliamentary elections, a local activist Märt Põder made a successful attempt of submitting an invalid vote. He also published his method. It was running the official voting client in a debugger and manipulating its memory until a vote containing an invalid candidate number was submitted. To check whether vote casting was successful or not, he used the official vote verification app that was not yet available in 2011. `https://www.ohtuleht.ee/664725/ainuke-e-haale-rikkuja-eestis-ei-julgeta-e-haaletamist-kritiseerida`

[5]Decision of Supreme Court in the case number 3-4-1-10-11. In Estonian. `https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-10-11`

electronic elections in Estonia was published by the city of Tallinn. Barbara Simons, a critic of electronic voting from the U.S., was invited to hold two public lectures. All these seemingly apolitical events were carried out with the involvement of the Central Party.[6]

Paavo Pihelgas set up his own website[7] where he offered a critical view on Estonian Internet voting. The negative media coverage about i-voting continued in 2012. Headlines such as "Developed countries avoid electronic voting" or "Shall we grant voting rights to computer viruses?" appeared in newspapers and the TV channel controlled by the Tallinn City Government which itself is controlled by the Central Party.[8]

Aftermath

How do those events fit into the attack tree with a root node "Change Result of Election Successfully"? The proof of concept malware developed by Paavo Pihelgas is seemingly closest to the actual manipulation attack and could be identified as a sub-attack "Attack Voting Equipment." There are some important characteristics missing from an actual manipulation attempt though. Pihelgas took great care not to perform any illegal activities. The malware only served to prove his point, there was no spreading mechanism and no stealth-techniques to avoid detection that one would except from a tool meant for actual attack. In fact – Pihelgas published the malware himself and actively sought public attention. His attempt still had the strong potential to "Change Result of Election Success- fully," but not through direct tampering with the Internet voting system, but through the revocation of the Internet voting results.

The problem with displaying candidates in the graphical user interface of the voting application was also used as a ground to apply for the revocation of the Internet voting results. It is interesting, that here it was not necessary for the candidate to develop the attack himself. It was enough to react to the technical and unintended bug, which was intentionally loaded with clearly political content. Similarly the attempted revocation by the Central Party was made possible by the events that they did not initiate themselves. The anti-i-voting movement initiated by them works towards diminishing the public confidence in Estonian Internet voting.

[6] To be precise, these events were organised by a specially-founded NGO Ausad Valimised (Honest Elections). The founding members of the NGO are closely related to the Central Party, even though formally the two organisations have nothing in common. The authors of the paper acknowledge that because of this precautious step the connection of the above-described events and the Central Party can be disputed.

[7] The original website `http://www.evalimised.net/` has since then gone offline, but an archived copy can be found at `https://web.archive.org/web/20110313034832/http://www.evalimised.net/`

[8] At the time of original writing (May 2013), 43 members out of 79 of the Tallinn City Council belonged to the Central Party. According to the Tallinn city budget published on May 15th , 2013, the support of Tallinn City Government to Tallinn TV in 2013 was EUR 2,980,000. According to the Estonian Business Register, 5 members out of 6 of Tallinn TV Council belonged to the Central Party as of May 20th, 2013.

Both the invalid i-vote and massive re-voting by one elderly woman remain mysterious to a certain extent. The elderly woman may have told the truth about her motivation, but there is also a possibility that somebody was testing the reaction of the voting system to anomalous events. There exists a possibility, that the invalid i-vote was due to a software error, there also exists a possibility, that the invalid i-vote was intentionally cast by someone who prefers to stay anonymous. If the latter is the case, then those events are similar to each other in a way that no attempt to hide the actions was taken. The difference from the revocation attempts is that no publicity was actively sought. All events mentioned so far contain no illegal steps which are characteristic to attacks that we normally would consider to activate the root node "Change Result of Election Successfully."

3.5 Attack Tree

3.5.1 Attacks to "Increase Influence on Society"

In order to find the primary threat for our attack tree it is necessary to analyse the motivation of an attacker. The purpose of an election is to delegate the power vested in the people to a small set of representatives. We are voters, candidates, observers and members of electoral committees during the elections. Between the elections we have different roles, but we still depend on the decisions made by those who were elected.

Any party affected by the political situation in the state, must be considered as an interested party and a possible attacker in the case of an election. An opposition party might be interested in winning the election and forming a government; a commercial enterprise might be interested in changing the taxation policies, or selling its voting technology; activists might be interested in getting some attention to those topics they consider important. All those groups are interested in increasing their influence on society, in order to implement policies consistent with their objectives.

A strategy for an opposition party trying to make it to the government would be to "Get enough seats in the parliament." It would also make sense to "Change the rules of election" in order to "Get enough seats in the parliament" in the next election for example by gerrymandering. The strategy of changing the rules of election could also be interesting for a voting technology provider looking for a market. In order to execute this strategy it would be useful to "Ruin election" to prove, that current election rules need changing. An attempt to "Ruin election" would also be useful to an activist group to bring public attention and media coverage to their members and themes. We argue that these three strategies – ("Get enough seats in the parliament," "Change the rules of election" and "Ruin election") – form the set of possibilities for a party who wants to use an election as a tool to increase its influence on society.

From here on we analyse threats to the voting method with respect to a rational attacker, interested in increasing its influence on society and therefore considering the three aforementioned strategies approach to the election. The

root node of our attack tree is "Increase influence on society." It is possible to represent all three strategies as attack trees. Some of the elementary nodes and branches in those trees are perfectly honest. An opposition party might "Get enough seats in parliament" by fair play. For threat modelling we consider dishonest branches of those attack trees which leads us to distinguish between the three categories of attacks – manipulation attacks, revocation attacks and attacks towards public confidence.

3.5.2 Manipulation Attacks

The goal of a manipulation attack is to change the election result in favour of the beneficiary by manipulating one of the voting results. A manipulation attack is targeted towards the integrity of a voting result. A successful manipulation attack gains at least one additional seat for the beneficiary in the parliament, whereas the fact that there was an attack must remain secret. Manipulation attacks are illegal.

In order to find possible vectors for manipulation attacks, we must analyse any actor, component, procedure or data of a voting method to understand how it affects the integrity of a voting result. First layers of the manipulation attack tree (see Figure 1) do not depend on the voting technology directly.

```
1. (OR) Manipulate the voting result
    1.1. (SUB) Replace ballot box before tabulation
    1.2. (SUB) Compromise tabulation tool
    1.3. (SUB) Forge the voting result
    1.4. (SUB) Prevent the tabulation of the result
    1.5. (OR) Break the integrity of the ballot box
        1.5.1. (SUB) Add votes to the ballot box
        1.5.2. (SUB) Remove votes from the ballot box
        1.5.3. (SUB) Modify votes in the ballot box
        1.5.4. (SUB) Break the availability of the ballot box
        1.5.5. (OR) Break the integrity of voters' votes
            1.5.5.1. (SUB) Vote on behalf of the voter
            1.5.5.2. (SUB) Coerce voter to vote in a certain way
            1.5.5.3. (SUB) Coerce voter not to vote
            1.5.5.4. (SUB) Prevent voter from voting
            1.5.5.5. (SUB) Disfranchise voter secretly
```

Figure 1: Manipulation attack tree

The nodes labelled as SUB are actually subtrees which define the possibilities to achieve this node in more detail. In those sub trees we already take the specifics of the voting method into account. We provide the sub tree "Vote on behalf of the voter" (see Figure 2) in the case of the Estonian Internet voting system as an example here.

```
1. (OR) Vote on behalf of the voter
    1.1. (LEAF) Manipulate voter's choice during voting
        (Malware attack)
    1.2. (LEAF) Manipulate display of voter's computer
        (Malware attack)
    1.3. (LEAF) Manipulate vote in transport channel (Attack
        transport channel)
    1.4. (LEAF) Manipulate list of candidates (Attack transport
        channel)
    1.5. (LEAF) Manipulate list of candidates (Attack central
        system)
    1.6. (LEAF) Hijack ID-card and PIN-codes (Malware attack)
    1.7. (LEAF) Forge ID-card (ID-card PKI)
    1.8. (LEAF) Steal ID-card and PIN-codes (Physical attack)
```

Figure 2: Vote on behalf of the voter

We consider the attacks in this sub tree elementary in the context of the Estonian Internet voting system, but they are not elementary *per se*. To "Manipulate voter's choice during voting" it is necessary to perform a possibly technology specific attack. When attacking voting technology, the assets belong to a voting method, but the attack technique itself is not voting specific. We have analysed those technology specific trees as well, because it is necessary to understand what it means to perform a malware attack (see Figure 3) against Internet voting for example. Please note that we are interested in the general structure of the attack and not the specifics of one or the other viral distribution method.

In addition to the malware attacks, we identified attacks against the transport channel, attacks against the central system and attacks against the ID-card PKI as technology specific attacks. We also developed an attack tree for coercive attacks, which in their general structure do not depend on the voting technology.

In the case of Estonian Internet voting, we haven't discovered any real manipulation attacks yet. The closest thing to a manipulation attack was the proof-of-concept malware written by Paavo Pihelgas. One version of this malware attempted to "Manipulate voter's choice during voting" and it used some techniques of a "Malware attack," but several characteristics of a "Malware attack" and manipulation attack were not met:

- The attack was meant to be shown publicly, not hidden;
- Great care was taken not to perform any illegal activity;
- The proof-of-concept malware did not use any stealth, distribution and anti-antivirus techniques characteristic to regular malware.

```
1. (AND) Malware attack
    1.1. (AND) Develop malware
        1.1.1. (AND) Acquire necessary knowledge about target
            1.1.1.1. (LEAF) Detect protocols used
            1.1.1.2. (LEAF) Detect protection mechanisms
            1.1.1.3. (LEAF) Detect interfaces used
        1.1.2. (AND) Create malware
            1.1.2.1. (LEAF) Modify existing malware
            1.1.2.2. (LEAF) Design new malware
        1.1.3. (LEAF) Execute malware in testing environment
    1.2. (OR) Distribute malware
        1.2.1. (LEAF) Use removable media
        1.2.2. (LEAF) Use viral mechanisms
        1.2.3. (LEAF) Use spoofing
        1.2.4. (LEAF) Use software patching infrastructure
        1.2.5. (LEAF) Distribute malware with hardware
        1.2.6. (OR) Use malware in those computers you control
            1.2.6.1. (LEAF) Use existing bot-net
            1.2.6.2. (LEAF) Compromise the organisation
    1.3. (OR) Launch an attack
        1.3.1. (LEAF) Send command to malware over some channel
        1.3.2. (LEAF) Malware regularly polls some resource for
            signal
        1.3.3. (LEAF) Use timer
```

Figure 3: Malware attack

3.5.3 Revocation Attacks

Revocation Attacks The goal of a revocation attack (Figure 4) is to change an election result in favour of the beneficiary by revoking one of the voting results. Revocation requires that there is a complaint by a voter, a candidate or a party about a violation of rights. In that case the National Electoral Committee has to consider, whether this violation is so widespread that it might affect the election result. If the answer is positive, a voting result can be revoked and a repeat vote must be held. The success of the attack depends on the voters' behaviour during the repeat vote.

A successful revocation attack gains at least one additional seat for the beneficiary in the parliament. A revocation attack is legal as long as the beneficiary did not perform the violation of the rights himself.

Revocation attacks make sense for several reasons. Firstly, if the violation of the rights can be attributed to supporters of a certain party, it is possible, that the repeat vote increases their turnout and provides additional seats for the party. Secondly, a parties' performance varies over voting methods. A party

```
1. (AND) Conduct a revocation attack
    1.1. (OR) Prove that rights of candidates or voters were
        violated
        1.1.1. (LEAF) Detect real violation of the rights
        1.1.2. (AND) Organise a violation of the rights
            1.1.2.1. (LEAF) Perform an attack against voters'
                rights
            1.1.2.2. (LEAF) "Discover" and publish violations
            1.1.2.3. (OR) Manage risks
                1.1.2.3.1. (LEAF) Avoid penalty
                1.1.2.3.2. (LEAF) Accept penalty
    1.2. (LEAF) Convince the NEC that the election result is
        affected
```

Figure 4: Conduct a revocation attack

Table 1: 2011 Parliamentary election voting results

	Total Voting result	Internet Voting Result
1	Reform Party (28.6%)	Reform Party (36.9%)
2	Central Party (23.3%)	Pro Patria and Res Publica Union (25.3%)
3	Pro Patria and Res Publica Union (20.5%)	Social Democrats (17.9%)
4	Social Democrats (17.1%)	Central Party (9.8%)

whose electorate prefers to vote in polling stations might not be popular in postal voting or Internet voting. This is clearly illustrated by the voting results tabulated during the 2011 Parliamentary election (Table 1).

If the Internet voting is stopped during the advance voting period due to some problems, all the i-votes are revoked and people are called to participate in Election Day voting in designated polling stations. The question is, how many of those i-voters will stay absent from the paper voting and would it have any real impact on the election result.

In the case of Estonian Internet voting, we have seen two attempts to revoke the Internet voting result and one attempt to revoke the election result. The attempt of Paavo Pihelgas was dismissed due to the fact that no actual violation of rights took place. The attempt of Henn Põlluaas was dismissed due to procedural problems. In the latter case it is possible to argue that a violation of the rights took place, but the NEC did not find that the election result was affected. All 3 voters who encountered the problem got help from the election hotline. The revocation attempt by the Central Party also built upon the hypothesis that the conditions for leaf-node "Detect real violation of the rights"

were met.

3.5.4 Attacks towards Public Confidence

The goal of an attack towards public confidence is to decrease trust towards a voting method. As a result, a significant fraction of the electorate may choose not to vote by a particular method, and as a consequence not to vote at all. Another possible aim of the attacks towards public confidence is to achieve cancelling of a voting method during future elections and hence efficiently get the same result as for the revocation attacks. Attacks towards public confidence are the most simple and risk-free attacks. It is enough to find a more or less hypothetical problem in the voting method and present it in a way that the public considers this a major issue (see Figure 5).

```
1. (AND) Damage the public confidence in a voting method
    1.1. (OR) Find a way to question the trustworthiness of a
        voting method
        1.1.1. (LEAF) Point out possible contradictions with the
            law
        1.1.2. (LEAF) Point out the problems from previous
            elections
        1.1.3. (LEAF) Exemplify the violation of election rules
    1.2. (OR) Work with the public
        1.2.1. (LEAF) Spread the message in the Internet
        1.2.2. (LEAF) Use public media
        1.2.3. (LEAF) Attend conferences
    1.3. (OR) Look for support
        1.3.1. (LEAF) Involve experts
        1.3.2. (LEAF) Involve political parties
        1.3.3. (LEAF) Involve the general public
    1.4. (AND) Involve institutions
        1.4.1. (LEAF) Submit a complaint to the electoral
            committee
        1.4.2. (LEAF) Submit a complaint to the Supreme Court
    1.5. (LEAF) Continue activity in-between the elections
```

Figure 5: Damage the public confidence in a voting method

It is difficult to distinguish this kind of an attack from the normal democratic process. The defence against these attacks is almost entirely the matter of public relations and the success depends on the value of the counter arguments. In the case of Estonian Internet voting, the problem is the lack of strong arguments. Specialists must admit that the malware is a real threat in this architecture, and there are no absolute controls for this threat.

Attacks towards public confidence mix sound arguments with demagogy and attempt to build an environment of distrust. From the viewpoint of the defenders, it is necessary to fulfil two tasks. Firstly, to recognise whether there are any real problems pointed out by the attacker. Secondly, to prevent the attack itself from going out of control.

The Internet voting related activity after the 2011 Parliamentary election is an example of a well-crafted attack towards public confidence – continuous negative media coverage is generated for i-voting, after the next election in 2013 it is possible to measure the success of the attack.

4 Discussion

Of these categories, manipulation attacks are the most studied ones. Our current election routines are a result of centuries of manipulation attempts and consequently adjusted regulations to keep the risk at an acceptable level and provide the electorate with the means to express their preferences in a fair manner.

It is probable that during the development of democratic practices certain parties also tried to discredit election principles as such, hence seeking to achieve a result favourable for them. However, a social agreement has been settled now for generations in democratic countries. Certain rules have been agreed upon concerning paper-based voting, and we follow them without thinking much about what exactly are their original roots.

The same does not hold for Internet voting. It is only in the last decade as the technology has become mature enough to support its practical deployment. Hence, it is almost inevitable that we see several disputes that the social memory has already forgotten about paper-voting issues, rising again in the context of Internet voting.

Since manipulation attacks are typically considered as the main threats against Internet voting, virtually all of the proposed solutions provide some level of protection against them. However, we claim that revocation attacks and attacks towards public confidence have got much less attention, and as a result we are much less protected against them.

Manipulation attacks have several problems. To gain an additional seat in the Estonian Parliament, it is necessary to get roughly an additional 5000 votes. Sometimes it is enough to gain only 50 more votes for an additional seat, but this is information that a potential beneficiary does not have at the moment when the decision to use a manipulation attack has to be made.

Manipulation attacks have to go unnoticed in order to be successful. This means that coercive attacks involving large numbers of voters are highly unlikely to succeed. An effective security engineering requirement can make technological attacks rather expensive. Voters' computers seem to be a low-hanging fruit, but the need to achieve an additional seat and to stay hidden makes a complex project.

The beneficiary considering a manipulation attack must also take into account the chance that the attack is discovered. Manipulation attacks are illegal; the consequences of getting caught should be severe for the reputation of the beneficiary. We do not know whether these difficulties are enough to prevent manipulation attacks from happening. The history of voting proves contrary. The risk of getting caught could be accepted by the beneficiary. It is possible to deny involvement after all and say that this is part of denigrate campaign against the beneficiary.

Revocation attacks are easier than manipulation attacks. It is possible to wait for a chance and try to show minor violations as major threats to an election result. Another possibility is to stage a violation. In the case of Internet voting, lot's of voters vote from computers they have received from their employers. At most times, the IT-department of the organisation has direct access to these computers. It is possible to plant malware on these computers and to "discover" it during the voting period. In case of revocation the attack can be considered successful, if the connection between the malware and the beneficiary stays secret. If the staging of the attack becomes known, the beneficiary's reputation is at risk.

For a successful revocation attack, the attacker still needs a large-scale manipulation of votes, which means that at least someone must break the law. This does not hold for the attacks towards public confidence. To harm the reputation of Internet voting, it is sufficient to raise reasonable suspicion in the electorate or the legislator. No real attack needs to be presented, just a proof- of-concept is sufficient. This means that attacks towards public confidence can be risk-free, yet cheap and efficient to perform. We argue that this makes them the most critical category of the three listed above.

5 Conclusion

The benefits of electronic and Internet voting have led researchers to look for ways of making electronic voting at least as transparent and observable as paper-based voting methods. Individually verifiable voting methods [Adi08, RBH$^+$09, Gjø10, PKRV10, GSB12] give additional tools to a voter to verify that at least some certain properties – e.g. cast as intended – hold on the vote cast by the voter. To achieve this property of verifiability, those schemes have to diverge from the straightforward implementations of a voting method. Verifiable voting schemes take advantage of additional communication channels and computational devices to avoid the need to completely trust one component of the system. Verifiable voting protocols often need those components to be under the control of parties who do not collude.

The complexity of verifiable voting schemes is justified by the added control – if the process of verification would indicate that her vote has been tampered with, the voter could turn to some other voting method instead and the principle of free elections would be enforced. Events with Estonian Internet voting in 2011 demonstrate the unsustainability of a trust-based voting model. The fact, that

there is no good way to answer manipulation attacks is a suitable ground for a successful attack on public confidence. Verifiability would help voters and electoral committees to counter those attacks.

Verifiability, if introduced, would be a new step in the process of voting, thus changing the voting model. We see it as a tool to counter manipulation attacks and attacks towards public confidence, but we have to analyse whether this new tool itself adds new ways to carry out attacks from any of the three categories from the threat model. It is obvious that any new components in the system can serve as new attack vectors against the system. From the experience with revoting we conclude that we have to take possible misuse of the tool into account. It is possible that malicious voters shall attempt to disrupt the election by falsely claiming that the verifiability indicates a manipulation with a vote, although there was none. If these voters cooperate, a new threat to trustworthiness of the elections rises which might give grounds to revocation attacks.

We conclude that threat modelling is an essential tool supporting the design of secure voting methods. By understanding the threats, we can state our requirements to the voting method more precisely. Threat modelling is a continuous process – an attempt to mitigate some threat by introducing new controls and changing the voting method must be followed by revisiting the threat modelling step. On the abstract level we need to answer one question: how does the proposed change to a voting method affect the set of possibilities to perform manipulation attacks, revocation attacks and attacks towards public confidence?

References

[ABO+03] Arne Ansper, Ahto Buldas, Mart Oruaas, Jaan Priisalu, Anto Veldre, Jan Willemson, and Kaur Virunurm. E-voting concept security: analysis and measures. Technical report, Estonian National Electoral Committee, 2003. Report number EH-02-01.

[Adi08] Ben Adida. Helios: Web-based Open-Audit Voting. In Paul C. van Oorschot, editor, *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 335–348. USENIX Association, 2008.

[BBD+05] Earl Barr, Matt Bishop, Dimitri DeFigueiredo, Mark Gondree, and Patrick Wheeler. Toward clarifying election systems standards. Technical report, Department of Computer Science University of California at Davis, 2005. Number CSE-2005-21.

[BFM04] Eric J Byres, Matthew Franz, and Darrin Miller. The use of attack trees in assessing vulnerabilities in SCADA systems. In *Proceedings of the international infrastructure survivability workshop*, pages 3–10, 2004.

[BM07] Ahto Buldas and Triinu Mägi. Practical Security Analysis of E-Voting Systems. In Atsuko Miyaji, Hiroaki Kikuchi, and Kai Rannenberg, editors, *Advances in Information and Computer Security, Second International Workshop on Security, IWSEC 2007, Nara, Japan, October 29-31, 2007, Proceedings*, volume 4752 of *Lecture Notes in Computer Science*, pages 320–335. Springer, 2007.

[cal01] Voting: What is, what could be, 2001. Caltech/MIT Voting Technology Project.

[CCF04] Sean Convery, David Cook, and Matthew Franz. An attack tree for the border gateway protocol, 2004. `https://tools.ietf.org/html/draft-ietf-rpsec-bgpattack-00`.

[DSTW12] Ardita Driza-Maurer, Oliver Spycher, Geo Taglioni, and Anina Weber. E-voting for Swiss Abroad: A Joint Project between the Confederation and the Cantons. In Manuel J. Kripp, Melanie Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting 2012, (EVOTE 2012), Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC, July 11-14, 2012, Castle Hofen, Bregenz, Austria*, volume P-205 of *LNI*, pages 173–187. GI, 2012.

[Gjø10] Kristian Gjøsteen. Analysis of an internet voting protocol. *IACR Cryptol. ePrint Arch.*, 2010:380, 2010.

[GSB12] Ida Sofie Gebhardt Stenerud and Christian Bull. When reality comes knocking norwegian experiences with verifiable electronic voting. In *5th International Conference on Electronic Voting 2012 (EVOTE2012)*, pages 21–33. Gesellschaft für Informatik eV, 2012.

[Har34] Joseph P. Harris. *Election Administration in the United States*. 1934.

[HJP05] Engelbert Hubbers, Bart Jacobs, and Wolter Pieters. RIES - Internet Voting in Action. In *29th Annual International Computer Software and Applications Conference, COMPSAC 2005, Edinburgh, Scotland, UK, July 25-28, 2005. Volume 1*, pages 417–424. IEEE Computer Society, 2005.

[HLW11] Sven Heiberg, Peeter Laud, and Jan Willemson. The Application of I-Voting for Estonian Parliamentary Elections of 2011. In Aggelos Kiayias and Helger Lipmaa, editors, *E-Voting and Identity - Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers*, volume 7187 of *Lecture Notes in Computer Science*, pages 208–223. Springer, 2011.

[Jon05] Douglas W. Jones. Threats to voting systems. a position paper, 2005. `http://homepage.cs.uiowa.edu/~jones/voting/nist2005.shtml`.

[JRSW04] David Jefferson, Aviel D Rubin, Barbara Simons, and David Wagner. A security analysis of the secure electronic registration and voting experiment (SERVE), 2004.

[JS12] Douglas W. Jones and Barbara Simons. *Broken Ballots: Will Your Vote Count? (Center for the Study of Language and Information).* 2012.

[KET10] Robert Krimmer, Andreas Ehringfeld, and Markus Traxl. The Use of E-Voting in the Austrian Federation of Students Elections 2009. In Robert Krimmer and Rüdiger Grimm, editors, *Electronic Voting 2010, EVOTE 2010, 4th International Conference, Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting.CC, July 21st - 24th, 2010, in Castle Hofen, Bregenz, Austria*, volume P-167 of *LNI*, pages 33–44. GI, 2010.

[KR05] Steve Kremer and Mark Ryan. Analysis of an Electronic Voting Protocol in the Applied Pi Calculus. In Shmuel Sagiv, editor, *Programming Languages and Systems, 14th European Symposium on Programming,ESOP 2005, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2005, Edinburgh, UK, April 4-8, 2005, Proceedings*, volume 3444 of *Lecture Notes in Computer Science*, pages 186–200. Springer, 2005.

[Kri12] Robert Krimmer. *The evolution of e-voting: why voting technology is used and how it affects democracy.* PhD thesis, Tallinn University of Technology, 2012.

[LDE11] Eric Lazarus, David L. Dill, and Jeremy Epstein. Applying a Reusable Election Threat Model at the County Level. In Hovav Shacham and Vanessa Teague, editors, *2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '11, San Francisco, CA, USA, August 8-9, 2011.* USENIX Association, 2011.

[LL07] Erik Loide and Ülle Lepp. E-voting - a Key to Independence for All. In Marion A. Hersh and James Ohene-Djan, editors, *Proceedings of the Conference and Workshop on Assistive Technologies for People with Vision and Hearing Impairments: Assistive Technology for All Ages (CVHI-2007), Granada, Spain, 28th - 31th August, 2007*, volume 415 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2007.

[MM06] Ülle Madise and Tarvi Martens. E-voting in Estonia 2005. The first Practice of Country-wide binding Internet Voting in the World. In Robert Krimmer, editor, *Electronic Voting 2006: 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC, August, 2nd - 4th, 2006 in Castle Hofen, Bregenz, Austria*, volume P-86 of *LNI*, pages 15–26. GI, 2006.

[MOP12] Guillermo Lopez Mirau, Teresa Ovejero, and Julia Pomares. The Implementation of E-voting in Latin America: The Experience of Salta, Argentina from a Practitioner's Perspective. In Manuel J. Kripp, Melanie Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting 2012, (EVOTE 2012), Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC, July 11-14, 2012, Castle Hofen, Bregenz, Austria*, volume P-205 of *LNI*, pages 213–224. GI, 2012.

[PC12] Tiphaine Pinault and Pascal Courtade. E-voting at Expatriates' MPs Elections in France. In Manuel J. Kripp, Melanie Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting 2012, (EVOTE 2012), Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC, July 11-14, 2012, Castle Hofen, Bregenz, Austria*, volume P-205 of *LNI*, pages 189–195. GI, 2012.

[PKRV10] Stefan Popoveniuc, John Kelsey, Andrew Regenscheid, and Poorvi L. Vora. Performance Requirements for End-to-End Verifiable Elections. In Douglas W. Jones, Jean-Jacques Quisquater, and Eric Rescorla, editors, *2010 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '10, Washington, D.C., USA, August 9-10, 2010*. USENIX Association, 2010.

[PLY11] J. Harold Pardue, Jeffrey P. Landry, and Alec Yasinsac. E-Voting Risk Assessment: A Threat Tree for Direct Recording Electronic Systems. *Int. J. Inf. Secur. Priv.*, 5(3):19–35, 2011.

[PYL10] J. Harold Pardue, Alec Yasinsac, and Jeffrey P. Landry. Towards Internet voting security: A threat tree for risk assessment. In *CRiSIS 2010, Proceedings of the Fifth International Conference on Risks and Security of Internet and Systems, Montreal, QC, Canada, October 10-13, 2010*, pages 1–7. IEEE Computer Society, 2010.

[RBH+09] Peter Y. A. Ryan, David Bismark, James Heather, Steve A. Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE Trans. Inf. Forensics Secur.*, 4(4):662–673, 2009.

[RCE+06] Mohammad S. Raunak, Bin Chen, Amr Elssamadisy, Lori A. Clarke, and Leon J. Osterweil. Definition and Analysis of Election Processes. In Qing Wang, Dietmar Pfahl, David M. Raffo, and Paul Wernick, editors, *Software Process Change, International Software Process Workshop and International Workshop on Software Process Simulation and Modeling, SPW/ProSim 2006, Shanghai, China, May 20-21, 2006, Proceedings*, volume 3966 of *Lecture Notes in Computer Science*, pages 178–185. Springer, 2006.

[RH08] Andrew Regenscheid and Nelson Hastings. A Threat Analysis on UOCAVA Voting Systems. Technical report, National

Institute of Standards and Technology, 2008. Report number NISTIR 7551, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7551.pdf.

[Sal88] Roy G. Saltman. Accuracy, Integrity and Security in Computerized Vote-Tallying. *Commun. ACM*, 31(10):1184–1191, 1218, 1988.

[Sch99] Bruce Schneier. Attack trees. *Dr. Dobb's journal*, 24(12):21–29, 1999.

[Sch00] Bruce Schneier. *Secrets & lies. Digital security in a networked world.* John Wiley & Sons., 2000.

[SGM+15] Uwe Serdult, Micha Germann, Fernando Mendez, Alicia Portenier, and Christoph Wellig. Fifteen years of internet voting in Switzerland [history, governance and use]. In *2015 Second International Conference on eDemocracy & eGovernment (ICEDEG)*, pages 126–132. IEEE, 2015.

[TIR09] Election Operations Assessment. Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA), 2009. https://www.eac.gov/sites/default/files/eac_assets/1/28/Election_Operations_Assessment_Threat_Trees_and_Matrices_and_Threat_Instance_Risk_Analyzer_(TIRA).pdf.

[VGRH81] William E Vesely, Francine F Goldberg, Norman H Roberts, and David F Haasl. Fault tree handbook. Technical report, Nuclear Regulatory Commission Washington DC, 1981.

[Vol09] Melanie Volkamer. *Evaluation of Electronic Voting - Requirements and Evaluation Procedures to Support Responsible Election Authorities*, volume 30 of *Lecture Notes in Business Information Processing.* Springer, 2009.

[Wei91] Jonathan D Weiss. A system security engineering process. In *Proceedings of the 14th National Computer Security Conference*, volume 249, pages 572–581, 1991.

[WV11] Komminist Weldemariam and Adolfo Villafiorita. Procedural security analysis: A methodological approach. *J. Syst. Softw.*, 84(7):1114–1129, 2011.

[YP11] Alec Yasinisac and J Harold Pardue. A process for assessing voting system risk using threat trees. *Journal of Information Systems Applied Research*, 4(1):4, 2011.