1

Introduction

1.1 Elections and Electronic Voting

Election History. The history of elections goes back a long way and election reforms have taken place several times: People in the ancient world wrote their decisions on shards, Englishmen in the Middle Ages cast their vote by public acclamation, Italians in the Renaissance used either polling bowls or polling stones, and voters in Prussia wrote their decisions in public electoral registers (compare to [42]). Starting at the end of the 19th century many, especially industrial, countries established the following election reforms: first, the principles of a *universal franchise* as well as a *direct* and *secret election* were introduced. Later, the principles of *free* and *equal suffrage* were added leading to the fact that women and poor people received the right to vote. In Germany all five principles have been explicitly embedded in the law since 1949 (compare to [122]). We might say that this can be considered as the beginning of modern democracy.

More recently, several countries all over the world have introduced further reforms: Postal voting and voting in advanced polling stations have been used to strengthen the universal franchise, though they weaken the secrecy of the vote and voter freedom. In Germany postal voting was integrated in the law in 1956, in Switzerland in 1991 (compare to [16]), and in Austria in 2008. Mechanical and later electronic voting machines were introduced to save money and time. In Germany, mechanical voting machines were integrated in the law in 1975 and electronic ones in 1999 (compare to [143]). In the U.S. the first mechanical lever machines were already in use in 1892 in New York and by the 1930's in all larger urban centres. The U.S. revolution of electronic voting began in the 1960's with the introduction of punch-card ballots, continuing with the introduction of optical mark-sense ballots and direct recording electronic (DRE) voting machines in the 1970's (compare to [131] for the American voting machine history).

In the beginning, electronic voting was limited to the use of electronic voting machines. Nowadays, we are more and more faced with the next major

M. Volkamer: Evaluation of Electronic Voting, LNBIP 30, pp. 1–10, 2009.

challenge: The introduction of remote electronic voting. This would enable voters to cast their vote over the Internet from any place and any device capable of connecting to the Internet (popular examples where remote electronic voting systems have already been used are Estonia and Switzerland).

Elections on Different Political Levels. With respect to governmental elections you can distinguish between local, provincial or national elections, and referenda. In addition, there exists many non-governmental elections: Examples include elections in companies, public authorities, organisations, societies, clubs, and associations, at universities and schools, as well as award nominations and general opinion surveys.

All these types of elections differ in their importance, degree of interest for manipulations, environment, and number of voters. Although the election principles apply to all of them, they are subject to different electoral laws. For instance, some elections on lower political levels have less stringent requirements with respect to the secrecy of the vote than governmental elections.

The general agreement in many countries is to gain experience with remote electronic voting on lower levels before going step by step towards more important elections until reaching the highest level (in Germany, the federal parliamentary elections). Thus, the technology should be tested in low level elections and can be improved if necessary; meanwhile the voters get used to the new technology and gain trust in it.

Electronic Voting as a Research Topic. The research community has investigated electronic voting since the early eighties. In 1981, one of the first technical research papers addressing electronic voting was published by David Chaum in [27]. Since then, numerous research papers have been published that propose cryptographic electronic voting approaches. Lists of publications in this area are available in [93], [90], and [59]. Blind signatures, homomorphic encryption, Mix networks, bit commitment, zero knowledge proofs, and threshold cryptography are only some examples of available cryptographic techniques. Most of them have been applied to solve the big challenge of providing unique voter identification (only eligible voters can cast a vote and those only once) and anonymous vote casting (the voter must be anonymous when he[1] casts a vote) at the same time. In later research papers, other aspects beside the pure voting protocol have been discussed, such as the trustworthiness of the voter's PC, Denial of Service attacks to the voting server, and temporary unlimited secrecy of the vote.

Besides this technical based research, electronic voting has also been analysed by other disciplines, including legal and social science. For instance, the time frame the secrecy of the vote must hold has been analysed from a legal point of view in [16], and a lot of research has been investigated on usability and accessibility issues of electronic voting systems (examples are [9] and [25]).

[1] Throughout this book the third person singular (him/he) is used as a gender neutral pronoun.

This research is as important as the technical literature because electronic voting is an interdisciplinary topic where people from different disciplines need to work together and learn from each other in order to successfully introduce electronic voting (see also [63]). This is reflected in many advisory boards for electronic voting projects where researchers from different scientific areas are represented. Also, the conference landscape has changed and conferences like the "Electronic Voting in Europe Workshop" in Bregenz were organised to hold an interdisciplinary and open discussion on all involved electronic voting issues.

Deployed Electronic Voting Systems. Beside the political, legal, and scientific developments, a huge variety of different electronic voting systems has been developed[2]. The most popular ones are the Diebold and Nedap electronic voting machines as well as the remote electronic voting systems POLYAS, VoteHere, Scytl, and T-Vote[3]. Such systems have been used for various elections all over the world on different political levels, both for trials and also for legally binding elections. Electronic voting machines have been used for parliamentary elections in countries like the U.S., the Netherlands, Belgium, France, Australia, Mexico, Brazil, Russia, and Germany. Remote electronic voting has been introduced in Switzerland, Estonia, the U.K., the Netherlands, Germany, France, and Austria, but on different political levels. In Estonia remote electronic voting is used for parliamentary elections countrywide, while in Germany it is implemented for elections in nationwide societies. A worldwide overview of countries where electronic voting machines as well as remote electronic voting systems have been applied is presented in [140].

In general, the systems in use are based on lower security techniques than the theoretical approaches published at various conferences. The deployed systems are easier to explain and to understand by the voter, while most of the theoretical available approaches require a rather technical and mathematical background. For instance, the Estonian electronic voting system can be explained easily as being the electronic copy of postal voting: The encryption of the vote corresponds to the inner envelope of postal voting, and the digital signature of the voter corresponds to the outer envelope (see [94] and Sect. 9.2 for more information). Thus, voters are rather convinced that this system works.

Activists. The introduction of electronic voting has not been embraced by everyone. Pressure groups[4] like Wij Vertrouwen Stemcomputers Niet[5] in the

[2] A list of electronic voting systems together with their links can be found in Sect. B.1.

[3] This paragraph might be a rather European or even German point of view.

[4] More information about these groups and their motivation can be found on their Web pages. Corresponding URLs are provided in Sect. B.2

[5] "Wij Vertrouwen Stemcomputers Niet" is Dutch and means "we do not trust voting computers".

Netherlands, the Chaos Computer Club (CCC) in Germany, the Verified Voting Foundation, and the Black Box Voting organisation in the U.S. as well as the group Irish Citizens for Trustworthy Evoting highly criticise electronic voting and are very sceptical with respect to the current electronic voting systems. They try to stop the usage of electronic voting in general and to prevent its introduction where politicians try to do so and they were even partly successful.

Responsible Election Authority. Despite the critical activist voices, "successful" hacking, and problems that have arisen, more and more responsible election authorities think about or have already decided to introduce electronic voting because of the manifold advantages it provides. Those advantages are, for instance, being more user-friendly, cost-effective and reliable, getting more accurate results and speed up the tallying time, as well as increasing the turnout by providing more mobility to the voter on election day. The responsible election authority naively believes that the insecure electronic voting systems are only those from other responsible election authorities or those from other countries. Thus, they argue that though the system might not be perfectly secure, first, the effort to hack the electronic voting system is too high compared to the importance of the election (for example, elections in societies), and, second, the paper-based system is also not one hundred percent secure. From their point of view electronic voting is acceptably secure without understanding all technical details. This problem has been addressed in literature (for instance in [102]), where the authors try to help the responsible election authority to "better understand the perspectives of electronic voting sceptics [..] to help them understand what the electronic voting sceptics are saying and why they are saying it, and to appreciate some of the questions about electronic voting technologies that worry many technologists".

1.2 Motivation

History shows that electronic voting cannot be stopped in our technically oriented society, where an increasing number of processes are mapped into the electronic world and voters become more and more mobile. Whenever people and in particular the responsible election authorities see the various advantages, they will start to implement electronic voting. It is only a question of time till electronic voting will be used for more and more elections and voters will become more aware of it. Maybe our grandchildren will not believe that we were used to use pen and paper to cast a vote and to go to a polling station (or even will not know anymore what a polling station is). Thus, it is essential to investigate how we can provide a *trustworthy base for secure electronic voting* in order to protect our democracy in the future and avoid the application of insecure electronic voting systems. Accidental as well as malicious abuse of electronic voting in our future election form must be prevented.

Considering the fact that the introduction of electronic voting has already started and a lot of problems with existing electronic voting systems have already been detected, the important questions are which of these existing *electronic voting systems are secure (enough)* to use them for a particular election and, related, how to design an electronic voting system that is secure (enough) for the application in certain elections. To answer these questions, the following two tasks are essential:

- First, the definition of the term "secure (enough)" for a particular election: as always in security, there is no 100% secure electronic voting system. Therefore, it needs to be defined whether a system is secure (enough) for a specific election in a certain environment; that is, under a certain *trust model.* Thus, a standardised, consistent, and exhaustive list of requirements for the electronic voting system which serves as basis for any evaluation, needs to be defined.

  Definition (Trust Model): In this book the definition of a trust model is divided into the following three aspects:
  - What are the assumptions about the environment?
  - What are the intruder's technical capabilities?
  - Who can be trusted not to maliciously cooperate with others?

  Note, a system that ensures the requirements regarding a minimised trust model, provides the most security, as the minimised trust model contains the lowest amount of assumptions and the maximised intruder's technical capability. Vise versa, the maximised trust model requires the highest amount of confidence in the environment and the lowest intruder's capability.
- Second, the assurance that a particular electronic voting system ensures these requirements under the defined trust model. Thus, a standardised *evaluation methodology*, which guides the evaluator how to check a given electronic voting system for a particular trust model. Elections are of individual importance, therefore it is essential to use an evaluation methodology which supports different evaluation depths and thus different assurance levels.

Having such a framework, the responsible election authority would need to define the underlying trust model and the assurance level. Based on this framework, a professional evaluator could examine a certain electronic voting system and decide whether it can be used in this context because it is secure enough or not.

1.3 Contribution, Methodology, and Structure

The contribution of this book is the development of such a framework for the evaluation of electronic voting systems. To reach this goal, four major

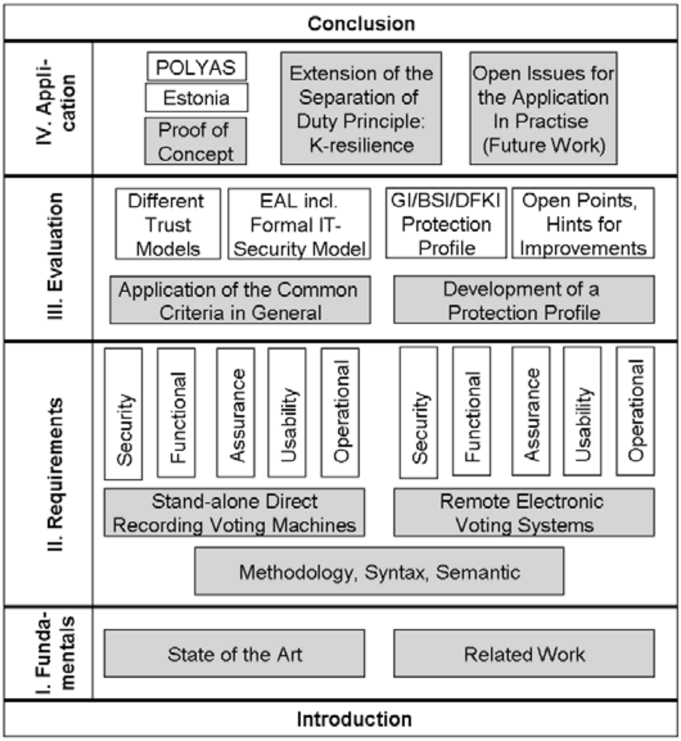
Conclusion
IV. Application
POLYAS
Estonia
Proof of Concept
Extension of the Separation of Duty Principle: K-resilience
Open Issues for the Application In Practise (Future Work)
III. Evaluation
Different Trust Models
EAL incl. Formal IT-Security Model
GI/BSI/DFKI Protection Profile
Open Points, Hints for Improvements
Application of the Common Criteria in General
Development of a Protection Profile
II. Requirements
Security
Functional
Assurance
Usability
Operational
Security
Functional
Assurance
Usability
Operational
Stand-alone Direct Recording Voting Machines
Remote Electronic Voting Systems
Methodology, Syntax, Semantic
I. Fundamentals
State of the Art
Related Work
Introduction

Fig. 1.1. Structure of the book

steps are taken, which correspond to the four main parts of this book (starting after this introduction chapter): Fundamentals, Requirements, Evaluation, and Application. Followed by these four parts, there is a conclusion part and an appendix. The contribution of each part, the applied methodology, and its structure are described in this section. Furthermore, the structure of the whole book is illustrated in Fig. 1.1.

- The **first part "Fundamentals"** provides the reader with a general introduction to the relevant issues of electronic voting and a critical discussion on available requirements and evaluation documents for electronic voting systems. Accordingly, this part is divided into the following two chapters:
  (A) In Chap. 2, the state of the art in electronic voting is proposed, analysed, and structurally reworked. A classification of election forms (including paper-based and electronic voting) and general differences between the latter two voting systems are worked out. Moreover, different implementations of the most common electronic voting machines in use, as well as remote electronic voting systems are described and discussed.

  (B) Chapter 3 discusses and analyses related work in terms of a couple of available lists of requirements and evaluation methodologies for electronic voting systems, which are conducted in so called requirement catalogues, corresponding laws, or regulations. Furthermore, scientific work concerning requirements for electronic voting is included in this discussion. The contribution is an overview of existing requirement documents, including the proposed evaluation methodology, and a list of vulnerabilities, which need to be overcome in the framework proposed in this book. In addition, some of the available requirement documents are identified as basis for the requirement definition in the second part of this book.

- The **second part "Requirements"** contributes a standardised, consistent, and exhaustive list of requirements for electronic voting systems. This list is detailed enough for the system developers to understand how their system can meet these requirements. In addition, the requirement list is deduced from legal input, so that lawyers accept these requirements. The provided list of requirements is not considered to be just another requirement catalogue but it is developed to improve and combine existing literature (which is referred to for each requirement). Therefore, a particular syntax and semantic is proposed and a particular methodology to develop the requirements is applied. This second part addresses two forms of electronic voting: stand-alone direct recording electronic voting machines and remote electronic voting systems. Correspondingly, this part is divided into the following three chapters:
  (A) Chapter 4 first describes the applied methodology to develop the standardised, consistent, and exhaustive list of requirements. The methodology includes cross checks against existing catalogues, the election principles, and possible threats. Furthermore, the necessity of defining different lists for different categories of electronic voting is explained. In addition, the language and notation for the requirement specification is defined in this chapter: a set of definitions for voting terminology and in particular for electronic voting specific items is presented. Moreover, the applied syntax and semantics are defined. This clarification enables a unique application of (electronic) voting specific items and a standardised language to ensure accuracy and contingency and, thus, to facilitate comparability.
  (B) The fist result of the development process – a standardised, consistent, and exhaustive list of requirements for stand-alone direct recording electronic voting machines – is provided in Chap. 5. This list contains system requirements (divided into functional, security, and usability requirements), organisational requirements, and assurance requirements.
  (C) The second standardised, consistent, and exhaustive list of requirements for remote electronic voting systems is provided in Chap. 6. As described for Chap. 5, this list contains system requirements (divided

into functional, security, and usability requirements), organisational requirements, and assurance requirements.

- The **third part "Evaluation"** contributes the proposal and discussion of a standardised evaluation methodology and certification procedure. This methodology accounts for the above defined security, functional, and assurance requirements, while it does not address operational and usability requirements. A further constraint concerns the type of electronic voting system: the evaluation methodology is elaborated for remote electronic voting systems. However, having defined a corresponding evaluation methodology, it can easily be adapted and/or extended for electronic voting machines or other forms of electronic voting.

  The developed evaluation and certification methodology provides a systematic and well defined compliance check for the selected requirements. In addition, the methodology provides impartial, comparable, and repeatable evaluation results, and is flexible with respect to the evaluation depth and the underlying trust model. Thus, arbitrary types of elections with their different trust models and different requirements to the evaluation depth can be handled. As it is not possible to handle all these options in one framework, a common basis framework for all remote electronic voting system evaluations is described. Accordingly, this part is divided into the following tow chapters:

  (A) Chapter 7 first analyses different existing IT security evaluation standards and shows that the Common Criteria [35] in combination with the Common Evaluation Methodology [36] works best for the evaluation and certification of remote electronic voting systems according to the defined security, functional, and assurance requirements. Second, this chapter applies the Common Criteria to remote electronic voting. This is done in the following four steps:

    - First, the Common Criteria itself is explained in detail and a mapping between the syntax used in the first part of the book and the Common Criteria language is provided.
    - In the next step, the role of a trust model for remote electronic voting in the context of the Common Criteria is discussed. A general as well as a detailed analysis id done for two essential remote electronic voting examples: the 'temporary unlimited secrecy of the vote' and the 'trustworthiness of the vote-casting device'. In this part, different possibilities to define the trust model are presented and the consequences for each possibility are presented.
    - The third step focuses on the evaluation depth. The previously identified assurance requirements for remote electronic voting systems are translated into the Common Criteria language.
    - The last step focuses on achieving high assurance levels: In this context, the Common Criteria requires a formal system specification and in particular a formal IT security model against which the system is evaluated. This is a first step to develop such a

formal IT security model for remote electronic voting systems. It covers an initial set of security and functional requirements. Note, formalising the previously defined security and functional requirements in a formal IT security model has more advantages than enabling corresponding Common Criteria evaluation depths: with the development of such a model the presented list of security and functional requirements can be validated or if necessary further improved by such a fundamental consistency check.

(B) Chapter 8 focuses on the completion of the evaluation framework. According to the Common Criteria, the security, functional, and assurance requirements are composed to a Protection Profile (a Common Criteria specific implementation-independent statements of security needs), however not a universal Protection Profile is provided but a core Protection Profile[6]. It is based on the lowest acceptable evaluation depth and the maximised trust model. This core Protection Profile should/has to be satisfied by any remote electronic voting system but can be extended if the trust model and/or the required evaluation depth change.

- The **fourth part "Application"** contains the application of two available remote electronic voting systems to the core Protection Profile and deduces open points within the application of the provided evaluation framework: it is shown that the third aspect of the trust model 'who can be trusted not to maliciously cooperate with others' is not sufficiently addressed by the core Protection Profile. Thi fourth part also proposes the remaining points for an application in practise. Correspondingly, the fourth part is *divided* into the following three chapters:

  (A) In Chap. 9, a proof of concept is executed to show the validity of the framework. Here, two remote electronic voting systems are analysed with respect to the previously developed core Protection Profile: the POLYAS system from Micromata and the Estonian remote electronic voting system, which was used for the parliamentary election in March 2007.

  (B) Chapter 10 concentrates on the separation of duty principle, which is neglected by the Protection Profile as it aims to be generic for the application of any voting protocol. An additional mechanism is developed to calculate how many entities need to maliciously cooperate in order to violate a particular security requirement: the calculation of the k-resilience value is introduced and is recommended as an extension to the Common Criteria certificate.

  (C) Chapter 11 addresses open issues for an evaluation of electronic voting systems in terms of future work.

[6] This core Protection Profile is based on the GI/BSI/DFKI Protection Profile [161].

The **conclusion** part closes the book with a summary of the contribution and implications for the trust in electronic voting systems. The **appendix** contains links to Web pages from electronic voting system vendors and electronic voting antagonists, the glossary, those requirements that are not considered, and the structure of a Protection Profile.