Design, Development, and Use of Secure Electronic Voting Systems

Dimitrios Zissis
University of Aegean, Greece

Dimitrios Lekkas
University of Aegean, Greece

A volume in the Advances in Electronic Government, Digital Divide, and Regional Development (AEGDDRD) Book Series

Information Science REFERENCE
An Imprint of IGI Global

Managing Director: Lindsay Johnston
Production Editor: Jennifer Yoder
Development Editor: Allison McGinniss
Acquisitions Editor: Kayla Wolfe
Typesetter: Lisandro Gonzalez
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Design, development, and use of secure electronic voting systems / Dimitrios Zissis and Dimitrios Lekkas, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-5820-2 (hardcover) -- ISBN 978-1-4666-5821-9 (ebook) -- ISBN 978-1-4666-5823-3 (print & perpetual access) 1. Electronic voting. 2. Electronic voting--Security measures. 3. Voting--Technological innovations. 4. Voting-machines--Technological innovations. 5. Political participation--Computer network resources. I. Zissis, Dimitrios, 1983- II. Lekkas, Dimitrios, 1969-
JF1032.D47 2014
324.6’5--dc23

2014003262

This book is published in the IGI Global book series Advances in Electronic Government, Digital Divide, and Regional Development (AEGDDRD) (ISSN: 2326-9103; eISSN: 2326-9111)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 4
A Holistic Framework for the Evaluation of Internet Voting Systems

Stephan Neumann
TU Darmstadt, Germany

Melanie Volkamer
TU Darmstadt, Germany

ABSTRACT

The foundations of democratic societies are elections. Due to their central importance to society, elections are bound to high legal standards, which are usually specified as election principles in national constitutions. To date, technological advance has reached elections, and Internet voting is a buzzword in the field of information technology. Many Internet voting systems and schemes have been proposed in research and some have even been used in legally binding elections. However, their underlying requirements are on the one hand often too closely linked to the specific technology and on the other hand mostly tailored to the scheme/system under investigation and therefore not connectable with election principles. This makes it difficult to compare different schemes/systems with each other, and correspondingly, it is difficult for election officials to select one of the proposed Internet voting schemes/systems for their own election setting. This chapter counters this artifact with two contributions, which are captured within an evaluation framework. First, based on the interdisciplinary method KORA, the authors derive constitutionally founded technical requirements. Second, they propose metrics to estimate the fulfillment of these requirements within concrete Internet voting systems. Given these contributions, the framework developed within this chapter supports election officials in making justified decisions about the selection and deployment of a specific Internet voting scheme/system.

DOI: 10.4018/978-1-4666-5820-2.ch004

INTRODUCTION

Elections build the basis of democratic societies and represent the exercise of popular sovereignty. The implementation of such a powerful means is therefore bound to high legal standards. Even though those standards might slightly differ depending on the specific national constitution and election type, all democratic states agree on three election principles namely *universal*, *equal*, and *free* according to the Universal Declaration of Human Rights (United Nations, 1948). Some states prescribe the deployment of even more election principles. For instance, the German Constitution anchors the principles of universal, equal, and free elections, but also requires the implementation of the *secret*, *direct*, and *public nature* principles.

With the rapid advance of modern communication technology elections have come into the focus of technical scientists; electronic voting has become a buzzword within the area of information and communication technology. The anticipated benefits of electronic voting are - amongst many others - the decrease of voter discrimination, the increase of voter turnout, the reduction of cost, and faster vote tallying. Starting with the seminal work by Chaum (1981), the challenge of voting over the Internet has been addressed by many researchers and many Internet voting schemes have been proposed to date, see for instance the works by Fujioka, Okamoto, and Ohta (1992), Juels, Catalano, and Jakobsson (2005), and Adida (2008). As opposed to purely theoretical considerations, several implementations of Internet voting schemes have found their way to practice and have been used for real-world elections, see for instance the presidential elections at the Université catholique de Louvain (Adida, de Marneffe, Pereira, & Quisquater, 2009) and the Estonian parliamentary elections (Maaten, 2005).

While the scientific literature often provides Internet voting schemes with proof (or at least strong evidence) for their security, the underlying security requirements are on the one hand too closely linked to the technology and on the other hand mostly tailored to the scheme under investigation. The same holds for other types of requirements such as functional and usability related requirements. Therefore, a legal evaluation of Internet voting systems and the resulting selection of adequate Internet voting systems with regard to the specific election setting seems hardly possible.

The goal of this work is to build a holistic evaluation framework that enables one to evaluate Internet voting systems according to the same requirements, i.e., the evaluation results for different Internet voting systems are comparable. Furthermore, the results are linked to election principles and thereby do not only cover security requirements. The evaluation of Internet voting systems according to this framework thereby leads to measurable outcomes, i.e. goes beyond existing approaches such as Common Criteria Protection Profiles which only allow statements about compliance or non-compliance of Internet voting systems and additionally only address security requirements.

In the remainder of this work, we first specify the target of evaluation, namely Internet voting systems. As election principles are too abstract to evaluate systems against, we deduced, in an interdisciplinary research project, a list of requirements that serve as basis for the evaluation of Internet voting system. We shall emphasize that the focus of this work is on the German Constitution. However, we explain how to adapt this work for other legal settings. The subsequent section is dedicated to the derivation of metrics for the determined requirements. These metrics are based on an extensive literature review. We additionally account for the importance of scientific literature in the field of Internet voting by outlining mappings between the requirements and metrics derived within, and the system properties and attacks widely known in the technical literature. We thereafter review

related literature and settle our own work in the research field and conclude this work and outline directions for future research.

Target of Evaluation: Internet Voting Systems

The focus of this work is on Internet voting systems rather than abstract Internet voting schemes. This is justified by the holistic approach of the proposed framework and by the fact that legal provisions cover technical issues that go beyond purely conceptual aspects; such system-dependent requirements are for instance system usability and system neutrality.

A clear understanding about the target of evaluation is important for every evaluation. The evaluation framework developed within this work is based on legal provisions. It is therefore important to understand what a voting system from a legal perspective is. In fact, from a legal perspective the conduction of the entire election must be implemented in a legally-compliant way. Given this, the evaluation of Internet voting systems cannot be purely conducted on the basis of specific aspects of the system such as the underlying cryptographic protocol. More practically speaking, it might be that one scheme is more secure than the other one but on the other hand not usable at all. Correspondingly, an evaluation purely on the cryptographic level is not sufficient.

Scientific research takes such considerations more and more into account; for instance Madise and Vinkel (2011) and Richter et al. (2013) with regard to the Estonian and German case respectively call for a more holistic consideration of electronic voting. More concretely, researchers have started taking the human/voter into account, such as Karlof et al. (2005), Tjøstheim et al. (2007), Ryan and Peacock (2005), Phan et al. (2012), Antoniou et al. (2007).

Based on recent work by Carlos et al. (2013) and following the legal considerations of Madise and Vinkel (2011), Richter et al. (2013) and the technical considerations of Tjøstheim et al. (2007), Ryan and Peacock (2005), Phan et al. (2012), Antoniou et al. (2007), we consider within our framework Internet voting systems as composition of three layers, namely the *human*, the *computer* (including hardware and software), and the *network* layer.

Derivation of Technical Requirements from Election Principles

The overall goal is to compare existing Internet voting systems on the level of election principles. However, these principles are abstract and as such must be made more concrete. Only then, can Internet voting systems be compared with respect to these concrete technical requirements.

We deduced technical requirements from the election principles relying on the interdisciplinary method KORA (Konkretisierung Rechtlicher Anforderungen, engl.: Concretization of Legal Requirements) invented by Hammer et al. (1993). KORA is a four-tier method for acquiring technical proposals based on legal provisions. On the first tier of KORA, application-specific *legal requirements* are identified from the relevant parts of the constitution, relevant constitutional court decisions, and the opportunities and risks of the technology under investigation. Afterwards the legal requirements are made more concrete to so-called *legal criteria* by considering simple law regulations and decisions from other courts[1]. For security-critical applications the list of legal criteria usually contains the *assurance* criterion, which defends against attackers trying to violate the other legal criteria. On the third tier, a language shift between the legal and technical language happens and technical expertise enters the process. Legal criteria are made more concrete to so-called *technical design goals* in an interdisciplinary dialogue. As input, existing technical documents are used together with the output of the previous layer. According to KORA, first *functional requirements*

are deduced and one further requirement is always derived from the universal legal criterion *assurance*, namely *system integrity.* This requirement implements the assurance criterion and ensures that all remaining technical requirements are deployed even in the case of adversarial presence. As such, system integrity builds a second layer upon the functional requirements, the *security layer*. We are well aware of the fact that the use of technical requirements in two dimensions might be counter-intuitive from a technical perspective. Richter (2012) elucidates the criterion assurance as follows: "*The assurance is a universal criterion that ensures the realization of all other criteria in the presence of intentional misbehavior and errors. […] For this purpose, there is need for a concept that secures the Internet voting system in its entirety*." Finally, on the fourth tier, a *technical design proposal* is deduced from the design goals. Due to the systematic deduction, this proposal is supposed to be constitutionally compliant. Note, the application of this method is not as straightforward as described herein. In particular on the third layer new concepts may come up and then legal scholars would go back to the second or even first layer to check whether this new aspect should be taken into consideration, or whether it cannot be justified by the laws and therefore should also not be taken into account on the other levels.

Richter et al. (2013) deployed the KORA method for Internet voting systems to derive 4 legal requirements and 10 legal criteria[2]. In an interdisciplinary project, we applied the KORA method on these legal criteria in order to derive technical requirements (called technical design goals in the KORA language). For the derivation of these technical requirements, we took as further input Volkamer's dissertation thesis (2009), which covers a broad set of technical requirements; this is justified by the fact that Volkamer reviewed for the derivation of technical requirements the German Regulations for Electronic Voting Machines (Federal Republic of Germany, 1999), the recommendations of the Council of Europe (2004), and the requirements of the catalogue by the Department of Metrological Information Technology in the National Metrology Institute (Hartmann, Meissner, & Richter, 2004).

The following 16 requirements have been deduced:

- **System Usability:** The voting system is usable to all eligible voters.
- **Accessibility:** The voting system is accessible to all eligible voters.
- **Vote Integrity:** The voting system ensures that each vote is correctly included in the election result.
- **System Availability:** The voting system is available to all eligible voters during the entire voting phase.
- **Voter Availability:** The voting system does not exclude eligible voters from casting their intention.
- **Eligibility:** The voting system ensures that only eligible voters' votes are included in the election result.
- **Uniqueness:** The voting system does not accept more than one vote per eligible voter.
- **System Neutrality:** The voting system does not influence the eligible voter's intention.
- **Fairness:** The voting system does not provide evidence about any eligible voter's intention before the end of the election.
- **Secrecy:** The voting system does not provide more evidence about an eligible voter's intention than the election result does.
- **Anonymity[3]:** The voting system does not reveal who participated in the election.
- **Individual Verifiability:** The voting system offers each eligible voter the possibility to verify that her intention has been correctly included in the election result.
- **Archiving:** The voting stores relevant data after the election.

- **Universal Verifiability:** The voting system offers any observer the possibility to verify that all technical requirements are enforced.
- **Accountability:** The voting system allows identifying the misbehaving party / parties in case of disputes resulting from the verifiability procedure.
- **Understandability:** The voting system is understandable to all voters.

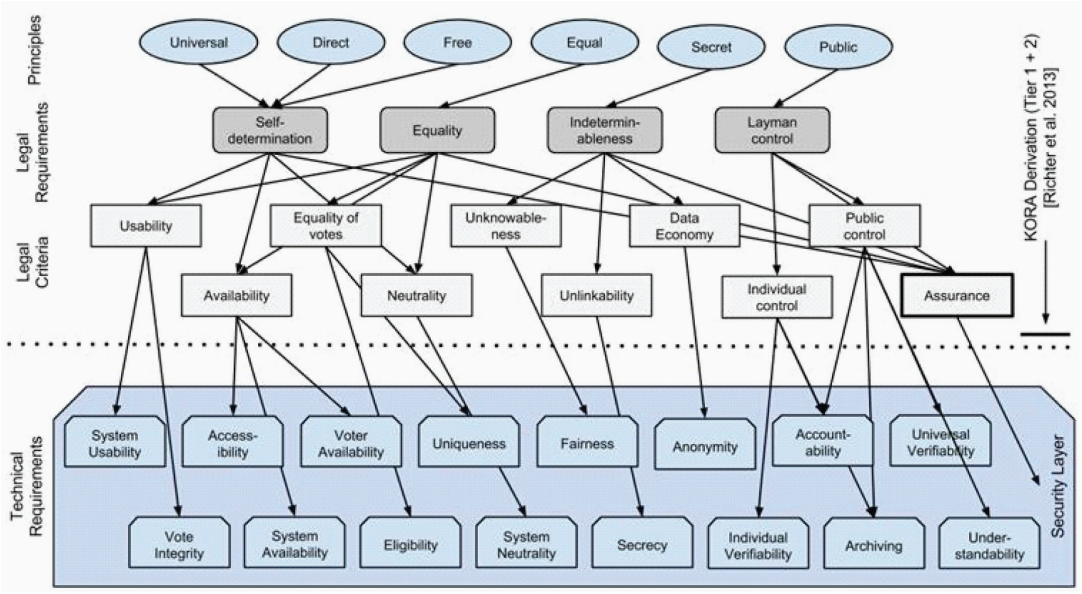
Given the awareness that some of the terms might be confusing as they often refer only to security aspects, we outline the functional layer for two of these exemplarily: From a functional perspective, secrecy indicates that the voting system must not reveal any voter's intention unintentionally, for instance by publishing a voter's name next to her cast intention on the bulletin board. On the functional layer, vote integrity indicates that the voting system must work correctly, i.e. for instance that the tallying algorithm tallies correctly.

An overview on the relation between technical requirements and their source election principles is provided in Figure 1. The herein derived technical requirements extend Volkamer's requirements, e.g., with regard to verifiability.

Measuring Technical Requirements

After abstract election principles have been converted into technical requirements, it shall be possible to evaluate voting systems against these requirements. In order to estimate to what extent Internet voting systems satisfy these requirements, it is necessary to specify how these technical requirements can be measured, i.e., metrics for the determined requirements have to be identified. In this section, we propose metrics to determine the degree of fulfillment of all technical requirements. These metrics depend on the type of technical requirement. On the functional layer, most of the 16 requirements require individual metrics, while on the security layer, the same approach for all 16 requirements can be applied. The herein proposed

Figure 1. Derivation of technical requirements from election principles. The requirement system integrity is depicted as separate layer on all other requirements.



metrics are the result of an extensive literature review using the terms from the identified requirements in combination with the terms *metric* or *standard* or *evaluation* or *measure*. Wherever possible, established metrics have been extracted from the literature. In case no established metrics are available, new metrics are proposed.

Measuring Functional Requirements

Among the most prevalent metrics to estimate *system usability* of voting systems, there are the ISO criteria (International Organization For Standardization, 1998), namely *effectiveness, efficiency,* and *satisfaction*. In accordance to the recommendations derived by Olembo and Volkamer (2013) we propose to evaluate system usability based on these three criteria (both for vote casting and verifying). As metrics we propose to measure effectiveness in terms of Boolean variables that indicate if voters succeed in voting, efficiency in terms of the time required to cast their vote, and satisfaction in terms of Sauro's score (2011) for the system usability scale (SUS) by Brooke (1996).

We propose to measure accessibility in terms of criteria derived within Voting System Performance Standards Summary (2013) and the US Election Assistance Voluntary Voting System Guidelines version 1.1 (2009). These criteria cover measures to enable voters with special capabilities. Following these guidelines, we evaluate how many of the following special-capabilities measures have been addressed throughout the development process: Low vision, blindness, special hearing capabilities, dexterity, language independence, and special cognitive capabilities.

As outlined in the derivation section, the requirements *vote integrity, voter availability*, *eligibility*, *uniqueness*, *fairness*, *secrecy*, and *anonymity* in terms of the functional layer are not typical functional requirements. Nevertheless, the underlying KORA methodology resulted in the two-layer concept of technical requirements. Rather than measuring these requirements in terms of quantification, we consider the functional layer of these requirements to be correctness requirements that any system shall ideally guarantee. Correspondingly, as metrics, we propose to measure all these requirements in terms of Boolean variables.

Extensive research has addressed the question of *system availability* with regard to Internet voting systems. Literature has proposed to estimate a voting system's availability "as the ratio of the time during which the system is operational (up time) to the total time period of operation (up time plus down time)" (National Institute of Standards and Technology, 2009). However, this information is only available after the elections. Correspondingly, it cannot be applied in advance to compare different Internet voting systems. We therefore propose measuring system availability according to the high-availability compendium (Bundesamt für Sicherheit in der Informationstechnik, 2013): the six availability classes for computing centers.

The *system neutrality* of an Internet voting system estimates the influence of the Internet voting system on the election result. We build the respective metric upon the works by Richter (Richter, 2012), the Recommendation Rec(2004)11 by the Council of Europe (2004), and the work by the Electoral Council of Australia & New Zealand (2013). As metrics, we propose to measure system neutrality in terms of Boolean variables. Note, the result depends on the concrete election setting because of the different colors that might be assigned to different parties, the concrete candidate list, etc.

The technical requirement of *individual verifiability* is composed of four sub-requirements (Budurushi et al., 2013), namely *encoded-as-intended*, *cast-as-encoded*, and *stored-as-cast*, and *tallied-as-stored* verifiability of an individual voter's vote. We therefore propose to measure individual verifiability of voting systems by the number of sub-requirements deployed in the voting system, whereas each sub-requirement is of equal value to the individual verifiability requirements.

Two ISO standards have been identified adequate to measure the extent to which the *archiving* requirement is satisfied. The standard for archiving of e*lectronic records* is the ISO 14721:2012 standard (International Organization For Standardization, 2012a), while the standard for the archiving of *general records* is the ISO 15489 standard (International Organization For Standardization, 2001). The Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC, 2007) provides metrics for the preservation of digital content, namely for the evaluation of the ISO 14721:2012 standard. These measures are standardized in the ISO 16363:2012 standard (International Organization For Standardization, 2012b) and cover the aspects *organizational infrastructure*, *digital object managements*, and *Technologies, Technical Infrastructure, & Security*. We propose to measure the requirement archiving of (electronic, non-electronic) documents with the cited checklists (TRAC, 2007), i.e. the ratio between satisfied and not satisfied items.

The technical requirement of *universal verifiability* covers the general public's possibility to verify the enforcement of all election principles (Richter, 2012, p. 147), particularly the correctness of the election result and the direct and secret elections principles (Richter, 2012, p. 319). We therefore propose to measure universal verifiability by the number of election principles, the enforcement of which can be verified by any observer (including the voters).

Accountability ensures that disputes resulting from verification procedures can be solved and misbehaving entities can be exposed. Accountability can be considered as super-criterion of verifiability (Küsters et al., 2010). In accordance to the individual and universal verifiability, we propose to estimate accountability in a voting system by the number of sub-requirements being accountable (refer to individual verifiability) and the number of election principles of which the violation can be attributed to someone (refer to universal verifiability).

Understandability is measured by the difference between voters' mental models of the system's functionalities, security properties and security model; and the actual system's functionalities, security properties and security model.

Measuring Security Requirements

A number of works derive requirements from concrete threats against which Internet voting systems are afterwards evaluated. We consider this approach inadequate for the proposed framework because the generic nature of this framework should not restrict the evaluation only to a restricted set of predefined threats. Rather, based on legally-founded but abstract security requirements, we propose to measure their degree of fulfillment by a *capability-based* approach (Amenaza Technologies Limited, 2005). Therefore, a list of adequate adversarial capabilities is required. We rely on the capabilities proposed by Neumann, Budurushi, and Volkamer (2014), which are categorized into communication-based, corruption-based, computational, and timing related capabilities. The capabilities derived by Neumann et al. are:

- **Communication-Based Capabilities:**
  - The adversary can drop messages from the network channel. (C1)
  - The adversary can read messages on the network channel. (C2)
  - The adversary can inject messages on the network channel. (C3)
  - The adversary can recognize the sender of messages on the network channel. (C4)
  - The adversary can notice the usage of a network channel. (C5)
- **Corruption-Based Capabilities:**
  - The adversary can corrupt a human entity. (C6)
  - The adversary can obtain objects from a voter. (C7)

  - The adversary can send objects to a voter. (C8)
  - The adversary can corrupt a computer system. (C9)
- **Computational Capabilities:**
  - The adversary is computationally unrestricted. (C10)
- **Timing Capabilities:**
  - The adversary has capability [1 - 10] during a specified period of time. (C11)

Building upon these capabilities, an Internet voting system's underlying security model is determined. Therefore, for each requirement, all possible compositions of capabilities that allow violating the investigated security requirement are determined. The simultaneous availability of any composition's capabilities must consequently be excluded (assumptions). The security model captures these assumptions in a term, which is often referred to as *k-resilience value* (Volkamer & Grimm, 2009). We propose to measure the security requirements by the corresponding k-resilience values.

Mapping

We are aware of the fact that technical requirements often used within the technical literature are different from the herein outlined requirements and adversarial capabilities. We therefore provide examples how our requirements and capabilities map to those used in other papers. The examples are mainly taken from literature of EVT 2008 and EVT/WOTE 2009-2012.

A number of works considers different forms of verifiability: Smyth et al. (2010) and Küsters et al. (2010) address the challenge of the general *public's possibility to verify* that online eligible voters cast votes. The technical requirements derived herein cover this aspect with the requirement universal verifiability and the fact that the security requirement eligibility is provided.

Chaum et al. (2008) outline *recording attacks* in which the voter might record herself during the vote casting process. In order to prevent secrecy violations by this kind of attacks, several voting systems must exclude the adversarial capability 2 (reading messages on the channel between the voter and the computer system), while other voting systems might only assume that one single vote casting process is unobserved, which results in the combined restriction of capabilities 2 and 10 (The adversary cannot read the channel between the voter and the computer system throughout the entire voting phase).

Benaloh (2008) outlines a *coercion attack* on Benaloh style ballot generation (Benaloh, 2006) if the coercer can interact with the voter during the ballot generation process and observe the network channel between the voter and the voting device. In such a case, the coercer might indicate to the voter when ballots should be challenged and when they should be cast. The verification information of challenged ballots would afterwards be handed out to the adversary such that the voter's only way not to get caught with "wrong" ballots would be if she always follows the adversary's will. In that case, the adversary would be assumed not to have capabilities 5 (noting whether the voter interacts with computer system), 7 (obtains challenged receipts from the voter), 8 (indicates when the vote is cast) simultaneously.

Several works (Essex, Clark, & Hengartner, 2012; Clarkson, Chong, & Myers, 2008; Grewal et al., 2013) build upon the JCJ voting scheme (Juels, Catalano, & Jakobsson, 2005) in order to defend against *simulation attacks*, in which the adversary forces the voter to forward her authentication material. Several schemes target at low-coercion elections and therefore assume that the adversary cannot gain the capabilities 8 (sending instructions to the voter) and 7 (receiving authentication material from the voter) simultaneously.

Benaloh (2008) and Popoveniuc et al. (2010) outline an attack that has later been outlined by Küsters, Truderung, and Vogt (2012) under the

name *clash attacks*. The idea of these attacks is that probabilistically encrypted votes are encrypted with the identical randomness such that identical votes lead to identical ciphertexts and identical receipts respectively. If receipts of different voters are identical, the adversary could decide to publish receipts that appear several times, only one time. In this case, the adversary is able to violate vote integrity. In the attack description by Küsters et al., the adversary is assumed not to have capability 9 (control the random generator in the voter's computer system and discard the vote).

A number of works (Sandler & Wallach, 2008; Moran & Naor, 2010; Demirel, Van De Graaf, & Araújo, 2012) outline *long-term attacks*, which allow the adversary to break secrecy by being computationally unrestricted. In their work, the authors address the problem that many voting systems rely on the assumption that the adversary cannot gain capability 10 (the adversary is computationally unrestricted).

RELATED WORK

The present work provides a holistic framework for the evaluation of Internet voting systems with respect to election principles. In preparation for the development of this framework, the literature has been studied and several related works have been identified. We review these works in the following and settle our own contribution to the field of research. The section is structured in accordance to the book chapter: First, related works proposing requirements for Internet voting are outlined; second, related works addressing the challenge of evaluating Internet voting systems are reviewed.

There are many documents proposing technical requirements for electronic voting such as the German Regulations for Electronic Voting Machines (Federal Republic of Germany, 1999), the recommendations of the Council of Europe (2004), the requirements of the catalogue by the Department of Metrological Information Technology in the National Metrology Institute (Hartmann, Meissner, & Richter, 2004), and the requirements catalogue by the German Informatics Society (Gesellschaft für Informatik, 2005). Those have not been systematically deduced from legal provisions. Moreover, most of them are taken into account when defining our requirements as Volkamer's work (2009) is used as basis. Mitrou et al. (2003) target at "*how an e-vote process should be designed and implemented in order to comply with the democratic election principles*." More concretely, they focus on the election principles of universal, free, equal, secret, and direct voting; additionally, they emphasize the importance of transparency, verifiability, accountability, security and accuracy. As opposed to our work, concrete technical requirements and corresponding metrics are not outlined. Rather, their focus is on measures and aspects to implement these election principles rather than on evaluation metrics for these principles.

The second branch of works studies the evaluation of Internet voting systems according to specified requirements[4]. The focus of previous work is on security evaluations. Volkamer (2009) lays the foundation for the development of a Common Criteria protection profile for Internet voting systems (Volkamer & Vogt, 2008). Further Internet voting system related protection profile drafts exist: Karokola, Kowalski, and Yngström (2012), and Lee et al. (2010) propose drafts for protection profiles taking verifiability into account. We essentially see three drawbacks which prevent the usage of PPs for our purposes: 1) The evaluation of systems according to PPs results in the system's compliance or non-compliance with regard to the PP, but does not yield fine-grained evaluation results. 2) Security objectives are generally not built upon legal derivations but rather rely on technical expertise in the field. 3) Assumptions about the environment can be freely posed and are subsequently not evaluated as outlined by Buchmann, Neumann, and Volkamer (2014). The second and third problems have been addressed by Schmidt

(2012) and Simić-Draws et al. (2013). Schmidt proposes a security concept template together with an evaluation, certification and accreditation approach for voting service providers. Schmidt builds upon the KORA method and Volkamer's technical requirements (2009) as evaluation criteria and recommends the usage of CC protection profiles and the IT Basic Protection as deployment measures. A similar but more general approach has recently been invented by Simić-Draws et al. (2013). The authors propose a holistic framework for the legally-justified security evaluation of IT systems. The authors therefore integrate the method KORA, the concept of CC protection profiles and the ISO 27001/IT-Grundschutz standard. As outlined above, the evaluation according to the CC and ISO 27001/IT-Grundschutz serves mainly as guideline to obtain security objectives and implement protective measures. Consequently, in case of non-compliance, the integrated framework does not foresee fine-grained evaluation results such that an ordering among the Internet voting systems cannot be obtained, in case further election specific constraints must be considered by election officials, such as for instance cost and performance. Similar security evaluation approaches as the one proposed in this work have been considered in the literature. Lazarus et al. (2011) develop a threat model capable of comparing different types of voting systems against each other. As opposed to our work, the authors consider the size of human conspiracies the only security metric rather than the compositions of more generic adversarial capabilities.

CONCLUSION

Elections build the foundation of democratic states and manifest the sovereignty of the people. Therefore, the voting ceremony is bound to rigorous election principles that are generally anchored in national constitutions. As one instance of a constitutional setting, this work is based on the six German election principles: universality, directness, freedom, equality, secrecy, and availability to the public.

In order to evaluate Internet voting systems with regard to election principles, those abstract principles were refined into technical requirements and evaluation metrics for these requirements were established. In conclusion, the present work provides a holistic framework that allows assessing the extent to which an Internet voting system complies with legal provisions. Thereby, the framework ultimately supports election officials in making justified decisions about the implementation of a specific Internet voting system for a specific election setting.

For the future we guide research into several directions: The present work restricts its focus on the evaluation of Internet voting systems with regard to the German legal setting. Extending the scope of the proposed framework for other electronic voting systems, such as electronic voting machines, and other legal settings can be done in future work. The KORA method takes both the concrete legal setting, and opportunities and risks of the technology under investigation, already in the first stage into account. As a consequence thereof, the extension requires reconsidering opportunities and risks throughout the requirements derivation with KORA. Furthermore, applying KORA on the basis of a different legal setting can be done by interdisciplinary collaboration between legal and technical scholars. Thereafter, metrics (if not listed within this work) can be derived by literature review. Concrete methodological processes shall be documented in order to provide evidence for the adequacy of the overall implementation of the herein proposed framework. Currently, we integrate the six election principles into the framework. Many types of voting systems however build upon electronic identification and authentication. As a consequence thereof, further basic rights have to be taken into account (in Germany but also in many other democratic states). In the future, we furthermore intend to identify election

specific constraints apart from legal constraints that influence the decision on which voting system is most appropriate for a specific election setting. These constraints might for instance cover the number of voters, authentication techniques in place, voters' devices, ballot types, and existing server infrastructure. Identifying high-level objectives and relevant constraints of election officials can be built upon established methodologies from economic sciences, such as value identification (Keeney, 2007). The present work proposes metrics for legally founded technical requirements. In the future, assurance levels have to be introduced in order to prove the evaluation's result reliability. For instance, k-resilience values might be derived by checking the system under investigation against identified threats or by the application of formal methods. Given the partially contradictory nature of election principles, voting systems cannot implement all election principles unconditionally. Consequently, impairments with regard to individual principles have to be accepted. The German constitution takes this fact into account and opens legal latitude when implementing Internet voting. It turns out that this legal latitude applies only on the level of election principles and cannot easily be transferred onto the level of technical requirements. In the future, the degree to which technical requirements are fulfilled must be propagated back to the layer of election principles.

ACKNOWLEDGMENT

This work has been developed within the projects "ModIWa2" – Juristisch-informatische Modellierung von Internetwahlen, which is funded by the Deutsche Forschungsgemeinschaft (DFG, German Science Foundation) and ComVote, which is funded by the Center for Advanced Security Research Darmstadt (CASED), Germany.

We also thank the reviewers for their valuable comments that helped to considerably improve the quality of this work.

REFERENCES

Adida, B. (2008). Helios: Web-based open-audit voting. In *Proceedings of USENIX Security Symposium*, (pp. 335-348). USENIX.

Amenaza Technologies Limited (2005). *Attack tree-based threat risk analysis*. Author.

Bannister, F., & Connolly, R. (2007). A risk assessment framework for electronic voting. *Int. J. Technology. Policy and Management*, *7*(2), 190–208.

Benaloh, J. (2006). Simple verifiable elections. In *Proceedings of the USENIX/accurate electronic voting technology workshop 2006 on electronic voting technology workshop*. USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1251003.1251008

Benaloh, J. (2008). Administrative and public verifiability: can we have both? In *Proceedings of the conference on electronic voting technology*. USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1496739.1496744

Bräunlich, K., Grimm, R., Richter, P., & Roßnagel, A. (2013). *Sichere Internetwahlen: Ein rechtswissenschaftlich-informatisches Modell*. Nomos. doi:10.5771/9783845246376

Brooke, J. (1996). SUS: A quick and dirty usability scale. In P. W. Jordan, B. Weerdmeester, A. Thomas, & I. L. Mclelland (Eds.), *Usability evaluation in industry*. Taylor and Francis.

Buchmann, J., Neumann, S., & Volkamer, M. (2014). Tauglichkeit von Common Criteria-Schutzprofilen für Internetwahlen in Deutschland. *Datenschutz und Datensicherheit-DuD*, *38*(2), 98–102. doi:10.1007/s11623-014-0040-x

Budurushi, J., Neumann, S., Olembo, M. M., & Volkamer, M. (2013). Pretty understandable democracy - A secure and understandable Internet voting scheme. In *Proceedings of 2013 Eighth International Conference on Availability, Reliability and Security (ARES)* (pp. 198-207). ARES. doi: 10.1109/ARES.2013.27

Bundesamt für Sicherheit in der Informationstechnik (2013). Hochverfügbarkeit-Kompendium Version 1.6, Band G, Kapitel 2: Definitionen. Author.

California Secretary of State (2013). *Voting System Performance Standards Summary*. Retrieved from http://www.sos.ca.gov/admin/regulations/proposed/elections/voting-systems/docs/voting-system-performance-standards-summary.pdf

Carlos, M. C., Martina, J. E., Price, G., & Custódio, R. F. (2013). An updated threat model for security ceremonies. In *Proceedings of the 28th annual ACM symposium on applied computing,* (pp. 1836–1843). New York, NY: ACM. doi:10.1145/2480362.2480705

Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R. L., & Sherman, A. T. (2008). Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *Proceedings of the conference on electronic voting technology*, (pp. 14:1-14:13). Berkeley, CA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1496739.1496753

Chaum, D. L. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, *24*, 84–90. doi:10.1145/358549.358563

Clarkson, M. R., Chong, S., & Myers, A. C. (2008). Civitas: Toward a secure voting system. In *Proceedings of IEEE Symposium on Security and Privacy*, (pp. pp. 354-368). IEEE Computer Society.

Cortier, V., Galindo, D., Glondu, S., & Izabachene, M. (2013). A generic construction for voting correctness at minimum cost - application to helios. *Cryptology ePrint Archive, Report 2013/177*.

Council of Europe (2004). *Legal, Operational and Technical Standards For E-Voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum*. Council of Europe Publishing.

Demirel, D., Van De Graaf, J., & Araujo, R. (2012). Improving Helios with everlasting privacy towards the public. In *Proceedings of the 2012 international conference on electronic voting technology/workshop on trustworthy elections*. USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2372353.2372361

Dreier, H. (2006). *Grundgesetz-Kommentar*. Morlok Siebeck Verlag.

Electoral Council of Australia & New Zealand (2013). *Internet voting in Australian election systems*. Retrieved from http://www.eca.gov.au/research/files/Internet-voting-australian-election-systems.pdf

Essex, A., Clark, J., & Hengartner, U. (2012). Cobra: toward concurrent ballot authorization for Internet voting. In *Proceedings of the 2012 international conference on electronic voting technology/workshop on trustworthy elections*. USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2372353.2372356

Federal Republic of Germany (1999). *Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland: Bundeswahlgeräteverordnung (BWahlGV)*. Retrieved from http://bundesrecht.juris.de/bundesrecht/bwahlgv/gesamt.pdf

Fujioka, A., Okamoto, T., & Ohta, K. (1992). A Practical Secret Voting Scheme for Large Scale Elections. In J. Seberry, & Y. Zheng (Eds.), *AUSCRYPT* (pp. 244–251). Springer.

Gesellschaft für Informatik (2005). *GI-Anforderungen an Internetbasierte Vereinswahlen*. Retrieved from https://www.gi.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf

Grewal, G. S., Ryan, M. D., Bursuc, S., & Ryan, P. Y. A. (2013). Caveat Coercitor: Coercion-evidence in electronic voting. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, (pp. 367-381). Washington, DC: IEEE Computer Society. Retrieved fromhttp://dx.doi.org/10.1109/SP.2013.32 doi: 10.1109/SP.2013.32

Hammer, V., Pordesch, U., & Roßnagel, A. (1993). *Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet*. Springer. doi:10.1007/978-3-642-78109-4

Hartmann, V., Meissner, N., & Richter, D. (2004). *Online Voting Systems for Non-parliamentary Elections - Catalogue of Requirements*. Laborbericht PTB-8.5-2004-1, Physikalisch-Technische Bundesanstalt Braunschweig und Berlin (Fachbereich Metrologische Informationstechnik). Retrieved from http://ib.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf

Institute of Electrical and Electronics Engineers (1998). *Standard for software test documentation* (Tech. Rep.). Retrieved from http://ieeexplore.ieee.org/xpls/abs\all.jsp?arnumber=741968

International Organization for Standardization (1998). *ISO 9241-11: Ergonomic requirements for office work with vdts: Guidance on usability*. ISO.

International Organization for Standardization (2001). *ISO 15489-1:2001: Information and documentation - records management part 1: General*. ISO.

International Organization for Standardization (2008). *ISO 9241-171: Ergonomics of human-system interaction: Guidance on software accessibility*. ISO.

International Organization for Standardization (2012a). ISO 14721:2012: Space data and information transfer systems -- Open archival information system -- Reference model. ISO.

International Organization for Standardization (2012b). ISO 16363:2012: Space data and information transfer systems -- Audit and certification of trustworthy digital repositories. ISO.

Juels, A., Catalano, D., & Jakobsson, M. (2005). Coercion-resistant electronic elections. In *Proceedings of ACM workshop on privacy in the electronic society*, (pp. 61-70). ACM. http://doi.acm.org/10.1145/1102199.1102213

Karlof, C., Sastry, N., & Wagner, D. (2005). Cryptographic voting protocols: A systems perspective. In *Proceedings of USENIX Security Symposium,* (LNCS), (vol. 3444, pp. 33–50). Springer-Verlag.

Karokola, G. R., Kowalski, S., & Yngström, L. (2012). Secure e-Government services: Protection Profile for Electronic Voting: A Case of Tanzania. In *Proceedings of IST Africa 2012 Conference*. IIMC International Information Management Corporation.

Keeney, R. L. (2007). Developing Objectives and Attributes. In *Advances in Decision Analysis*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511611308.008

Küsters, R., Truderung, T., & Vogt, A. (2010). Accountability: definition and relationship to verifiability. In *Proceedings of the 17th ACM conference on computer and communications security*, (pp. 526-535). New York, NY: ACM. doi: 10.1145/1866307.1866366

Küsters, R., Truderung, T., & Vogt, A. (2012). Clash Attacks on the Verifiability of E-Voting Systems. In *Proceedings of IEEE Symposium on Security and Privacy (S&P 2012),* (pp. 395-409). IEEE Computer Society.

Lazarus, E. L., Dill, D. L., Epstein, J., & Hall, J. L. (2011). Applying a reusable election threat model at the county level. In *Proceedings of the 2011 conference on electronic voting technology/workshop on trustworthy elections*, (p. 12). Berkeley, CA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2028012.2028024

Lee, K. W., Lee, Y., Won, D., & Kim, S. (2010). Protection Profile for Secure E-Voting Systems. In *Proceedings of ISPEC*, (pp. 386-397). Springer.

Madise, Ü., & Vinkel, P. (2011). Constitutionality of remote Internet voting: The Estonian perspective. *Juridica International, 18*.

Mitrou, L., Gritzalis, D., Katsikas, S. K., & Quirchmayr, G. (2003). Electronic voting: Constitutional and legal requirements, and their technical implications. In D. Gritzalis (Ed.), *Secure electronic voting*, (Vol. 7, pp. 43-60). Springer. Retrieved from http://dblp.uni-trier.de/db/series/ais/ais7.html#MitrouGKQ03

Moran, T., & Naor, M. (2010). Split-ballot voting: Everlasting privacy with distributed trust. *ACM Trans. Inf. Syst. Secur., 13* (2), 16:1-16:43. doi: 10.1145/1698750.1698756

National Institute of Standards and Technology (2009). Draft Voluntary Voting System Guidelines Version 1.1, Volume I: Voting System Performance Guidelines. Author.

Neumann, S., Budurushi, J., & Volkamer, M. (2014). Analysis of security and cryptographic approaches to provide secret and verifiable electronic voting. In D. Zissis, & D. Lekkas (Eds.), *Design, development, and use of secure electronic voting systems*. Hershey, PA: IGI Global.

Neumann, S., Kahlert, A., Henning, M., Richter, P., Jonker, H., & Volkamer, M. (2013). Modeling the German legal latitude principles. In *Proceedings of ePart* (pp. 49–56). Springer.

Olembo, M. M., & Volkamer, M. (2013). E-Voting System Usability: Lessons for Interface Design, User Studies, and Usability Criteria. In S. Saeed, & C. Reddick (Eds.), *Human-Centered System Design for Electronic Governance* (pp. 172–201). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-3640-8.ch011

Phan, H., Avrunin, G., Bishop, M., Clarke, L. A., & Osterweil, L. J. (2012). A systematic process-model-based approach for synthesizing attacks and evaluating them. In *Proceedings of the 2012 international conference on electronic voting technology/workshop on trustworthy elections*, (p. 10). Berkeley, CA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2372353.2372363

Popoveniuc, S., Kelsey, J., Regenscheid, A., & Vora, P. (2010). Performance requirements for end-to-end verifiable elections. In *Proceedings of the 2010 international conference on electronic voting technology/workshop on trustworthy elections*, (pp. 1-16). Berkeley, CA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1924892.1924903

Richter, P. (2012). *Wahlen im Internet rechtsgemäß gestalten*. Nomos. doi:10.5771/9783845243450

Richter, P., Bräunlich, K., Grimm, R., & Roßnagel, A. (2013). *Sichere Internetwahlen - Ein rechtswissenschaftlich-informatisches Modell*. Nomos.

Ryan, P. Y. A., & Peacock, T. (2005). *Prêt à Voter: a Systems Perspective* (Tech. Rep.). School of Computing Science, Newcastle University. Retrieved from http://www.cs.newcastle.ac.uk/publications/trs/papers/929.pdf

Sandler, D. R., & Wallach, D. S. (2008). The case for networked remote voting precincts. In *Proceedings of the conference on electronic voting technology*, (pp. 6:1-6:7). Berkeley, CA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1496739.1496745

Sauro, J. (2011). *Measuring Usability With The System Usability Scale (SUS)*. Retrieved from http://www.measuringusability.com/sus.php

Simić-Draws, D., Neumann, S., Kahlert, A., Richter, P., Grimm, R., Volkamer, M., & Roßnagel, A. (2013). Holistic and Law Compatible IT Security Evaluation: Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA. [IJISP]. *International Journal of Information Security and Privacy*, *7*(3), 16–35. doi:10.4018/jisp.2013070102

Smyth, B., Ryan, M. D., Kremer, S., & Kourjieh, M. (2010). Towards automatic analysis of election verifiability properties. In *Proceedings of Arspawits'10: Joint workshop on automated reasoning for security protocol analysis and issues in the theory of security*, (Vol. 6186, pp. 165-182). Springer. Retrieved from http://www.bensmyth.com/files/Smyth10-towards-definition-verifiability.pdf

Tjøstheim, T., Peacock, T., & Ryan, P. Y. A. (2007). *A case study in system-based analysis: The Threeballot voting system and Prêt à Voter*. Academic Press.

Trustworthy Repositories Audit & Certification (2007). *The Trustworthy Repositories Audit & Certification: Criteria and Checklist*. Retrieved from http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

United Nations (1948). *The universal declaration of human rights*. Retrieved from http://www.un.org/en/documents/udhr

US Election Assistance (2009). *Voluntary Voting System Guidelines*. Retrieved from http://www.eac.gov/assets/1/AssetManager/VVSG_Version_1-1_Volume_1_-_20090527.pdf

Volkamer, M., & Grimm, R. (2009). Determine the Resilience of Evaluated Internet Voting Systems. In *Proceedings of REVOTE*, (pp. 47-54). IEEE Computer Society. ISBN: 978-0-7695-4100-6

Volkamer, M., & Vogt, R. (2008). *Basic set of security requirements for Online Voting Products BSI-CC-PP-0037*. Federal Office for Security in Information Technology.

KEY TERMS AND DEFINITIONS

Adversary Capabilities: The list of capabilities that an adversary might possess and might use to violate a security requirement.

Functional Requirements: The 16 requirements an Internet voting system shall satisfy independent of an adversarial presence.

German Election Principles: The six principles of universal, direct, free, equal, secret, and public elections that are anchored in the German Constitution.

Security Requirements: The 16 requirements building a security layer upon the functional requirements, i.e. security requirements ensure the enforcement of functional requirements in the presence of adversaries.

ENDNOTES

[1] Note, a re-running of this method for other countries becomes essential to fit the specific constitutional and legal setting because of the different simple law regulations and court decisions.

[2] As opposed to Richter et al., the present work is restricted to constitutional election principles. This decision is justified by the fact that further legal provisions, such as the Right to Informational Self-Determination and Secrecy of Telecommunications, are too specific to a concrete legal setting and therefore beyond the scope of this work this work.

[3] Besides Germany there are other countries such as France requiring hiding the information, who participated in the election and who not as outlined by (Cortier et al., 2013). However, we are also aware that applying KORA in other countries this requirement would not necessarily be included, such as in Belgium due to compulsory voting.

[4] Note, literature on evaluation also defines requirements against which the systems are evaluated.