Evaluation von Internetwahlsystemen

Melanie Volkamer

Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt
Mornewegstraße 32; 64293 Darmstadt
volkamer@cased.de

Abstract: Seit einiger Zeit wird unsere Gesellschaft immer mobiler. Durch den Einsatz des Internets bei Wahlen kann diesem Wandel Rechnung getragen werden. Damit die Demokratie durch Internetwahlen nicht gefährdet wird, müssen die entsprechenden Systeme positiv evaluiert werden. Hierzu wird ein standardisierter, umfassender und in sich konsistenter sowie produktunabhängiger Anforderungs- und Evaluierungskatalog entwickelt, der auf der Methodik der Common Criteria beruht. Dieser Katalog wird auf existierende Systeme angewendet. Eine dabei aufgedeckte Schwachstelle der Common Criteria wird durch einen eigenen Ansatz geschlossen.

1 Einführung

In Deutschland fanden seit Anfang des 19ten Jahrhunderts verschiedene Wahlreformen statt. Hierzu zählen unter anderem die Erteilung des Wahlrechts an Frauen, die Einführung der Briefwahl und die Ausdehnung des Kommunalwahlrechts auf Ausländer. Diese Reformen verdeutlichen, dass das Wahlrecht immer wieder neuen kulturellen Gegebenheiten angepasst wurde. Seit einigen Jahren zeichnet sich ein neuer kultureller Wandel in der Gesellschaft ab: Die Wähler werden immer mobiler und wohnen oft temporär im Ausland. Diese Wähler müssen derzeit die Briefwahl nutzen, um überhaupt an der Wahl partizipieren zu können und das funktioniert auch nur, wenn sie diese frühzeitig beantragen und zurückschicken. Diese Aufwände und zeitlichen Randbedingungen führen zu einer sinkenden Wahlbeteiligung. Dem kann entgegengewirkt werden, wenn man die Internetwahl parallel zur Briefwahl ermöglicht. Hier kann der Wähler noch am Wahltag seine Stimme abgeben und braucht keinen Antrag auf Zusendung von Wahlunterlagen zu stellen. Zusätzlich kann das Internetwahlsystem den Wähler auf Fehler beim Ausfüllen des Stimmzettels hinweisen und ermöglicht eine schnelle Auszählung der Stimmen.

Motiviert durch diese Vorzüge werden Internetwahlen seit Ende der neunziger Jahre erforscht und erprobt, z.B. bei den Wahlen der Gesellschaft für Informatik und der Deutschen Forschungsgemeinschaft sowie bei den Nationalratswahlen in Estland und den Niederlanden. Otto Schily förderte diese Aktivitäten mit dem Ziel zur Bundestagswahl 2006 Internetwahlen einzusetzen. Dieses Ziel wurde nicht erreicht und auch die Wahl 2009 wird ohne Internetwahlen abgewickelt. Ausschlaggebend sind Bedenken bzgl. der Sicherheit, denn die Frage, ob ein Internetwahlsystem für eine bestimmte Wahl sicher genug ist, kann

derzeit nur sehr unbefriedigend beantwortet werden. Zwar wurden von verschiedenen Organisationen wie dem Europarat und der Gesellschaft für Informatik Anforderungskataloge für Internetwahlsysteme erstellt, hier wird aber nicht festgelegt, wie und auf Basis welchen Vertrauensmodells die Konformität mit den Anforderungen nachzuweisen ist.

An dieser Stelle setzt dieser Beitrag an. Hierzu werden in Kapitel 2 zunächst existierende Anforderungskataloge für elektronische Wahlsysteme untersucht und anschließend wird erläutert, wie darauf aufbauend ein umfassender und in sich konsistenter Anforderungskatalog für Internetwahlsysteme entwickelt wurde. Die Anforderungen aus diesem Katalog werden im dritten Kapitel in die Methodik der Common Criteria (CC) übersetzt und eine dabei aufgedeckte Schwachstelle der Common Criteria durch einen eigenen Ansatz geschlossen. Im vierten Kapitel wird der entstandene standardisierte und produktunabhängige Evaluierungskatalog auf zwei Internetwahlsysteme angewendet. Der Beitrag schließt im fünften Kapitel mit einem Ausblick und einer Zusammenfassung.

2 Anforderungskatalog

Existierende Anforderungskataloge. Es werden drei Klassen von Anforderungskatalogen unterschieden: Solche, die in einem Anwendungskontext entstanden sind und entweder Wahlgeräte oder Internetwahlsysteme adressieren, und solche, die in einem eher wissenschaftlichen Kontext entstanden sind.

Untersucht wurden die folgenden Anforderungskataloge für Wahlgeräte: Bundeswahlgeräteverordnung, Richtlinien für den Einsatz des Digitalen Wahlstift-Systems und verschiedene amerikanische Verordnungen, wie die der Federal Election Commission, dem Help America Vote Act und der IEEE.

Des Weiteren wurden folgende Anforderungskataloge für Internetwahsysteme analysiert: Empfehlungen des Europarates, der Anforderungskatalog der Gesellschaft für Informatik, der Anforderungskatalog für Online-Wahlsysteme der Physikalisch-Technischen Bundesanstalt, Wahlgesetze aus der Schweiz und Österreich und der Network Voting System Standard aus den USA.

Neben diesen Ansätzen aus der Praxis wurden die folgenden wissenschaftlichen Arbeiten untersucht: Shamos' Commandments, die Doktorarbeiten von Mercuri und McGaley sowie Veröffentlichungen zum Thema Anforderungen aus dem EU Cyber Vote Projekt.

Die Analyse deckt eine Reihe von Schwachstellen der existierenden Anforderungskataloge auf: Einige Anforderungen sind nicht eindeutig oder gar widersprüchlich formuliert und der Detailierungsgrad schwankt innerhalb eines Kataloges. Keiner der Anforderungskataloge erfüllt den Vollständigkeitsanspruch. Darüber hinaus wird weder das Evaluierungsverfahren noch die Evaluierungstiefe explizit spezifiziert. Ebenso wird auch das zugrunde liegende Vertrauensmodell nicht festgelegt. Dies hat zur Folge, dass auf Grundlage der existierenden Kataloge für ein System nicht eindeutig entschieden werden kann, ob es die Anforderungen erfüllt oder nicht. Insgesamt ist festzustellen, dass damit bisher kein umfassender, standardisierter und in sich konsistenter sowie produktunabhängiger Anforderungskatalog und auch kein aussagekräftiges Evaluierungsverfahren existiert. Als Konse-

quenz ist festzuhalten, dass die bisher erzielten Evaluierungsergebnisse nicht vergleichbar sind.

Umfassender und in sich Konsistenter sowie Produktunabhängiger Anforderungskatalog. Aufbauend auf diesen Ergebnissen wurde zunächst ein umfassender und konsistenter sowie produktunabhängiger Anforderungskatalog für Internetwahlsysteme[1] entwickelt, der die identifizierten Schwachstellen bei der Definition der Anforderungen beseitigt. Dieser Katalog beinhaltet neben den sicherheitsspezifischen und funktionalen Anforderungen auch organisatorische Anforderungen sowie Anforderungen an die Benutzerfreundlichkeit und die Vertrauenswürdigkeit. Da hier aus Platzgründen nicht der gesamte Anforderungskatalog dargestellt werden kann (Abbildung 1 zeigt ein Beispiel), liegt der Fokus auf der Methodik zur Entwicklung dieses Kataloges:

Hierzu wurde zu nächst der Evaluierungsgegenstand genau definiert: Es werden Internetwahlsysteme betrachtet, die es dem Wähler ermöglichen, sich zu identifizieren und zu authentifizieren, eine Kandidatenauswahl zu treffen und diese beliebig oft zu verändern bis die Stimme endgültig abgegeben ist. Dabei werden weder Verifizierbarkeitsfunktionen für den Wähler[2] noch ein Stimm-Updating (d.h. der Wähler kann seine elektronische Stimme beliebig oft aktualisieren und nur die letzte Stimme wird gezählt) betrachtet. Um die Produktunabhängigkeit zu erreichen, wurde versucht so viele technische und insbesondere kryptographische Ansätze wie möglich zu berücksichtigen. Insbesondere bzgl. des Wahlgeheimnisses werden Systeme, die MIXe, homomorphe Verschlüsselung, blinde Signaturen oder Secret Sharing verwenden, adressiert.

Um die Konsistenz der Anforderungen sicherzustellen, wurde ein Glossar für Wahl- und insbesondere elektronische Wahlterminologie entwickelt und eine eigene Syntax und zugehörige Semantik vorgeschlagen.

Um sicherstellen zu können, dass die Anforderungen möglichst vollständig sind, wurden die folgenden Prozesse durchlaufen: Zunächst wurde eine Bedrohungsanalyse [Sto96] durchgeführt, um alle denkbaren Angriffe durch entsprechende Anforderungen abwehren zu können. Anschließend wurde die KORA Methode zur Konkretisierung rechtlicher Anforderungen [HPR92] eingesetzt, damit die unterschiedlichen Aspekte der Wahlrechtsgrundsätze in den Anforderungen berücksichtig werden. Des Weiteren wurde sichergestellt, dass Anforderungen aus existierenden Katalogen in den Anforderungskatalog einfließen. Hierzu wird in den Anforderungen auf existierende Kataloge verwiesen[3].

[1] In [Vol09] wird zunächst ein Anforderungskatalog für Wahlgeräte entwickelt und aufbauend auf diesem ein zweiter Katalog für Internetwahlsysteme.

[2] Zwar hat das Bundesverfassungsgericht mit seinem Urteil vom 3. März 2009 die Wichtigkeit der Kontrollierbarkeit durch den Wähler betont, aber auch eingeräumt, dass diese zu Gunsten anderer Wahlrechtsgrundsätze eingeschränkt werden kann. Dies ist bei Internetwahlen der Fall, da diese parallel zur Briefwahl eingesetzt werden und damit dazu dienen, das Prinzip der allgemeinen Wahl zu stärken.

[3] Dies geschieht für die drei wichtigsten Anforderungskataloge [Cou04], [HMR04] und [Ver99].

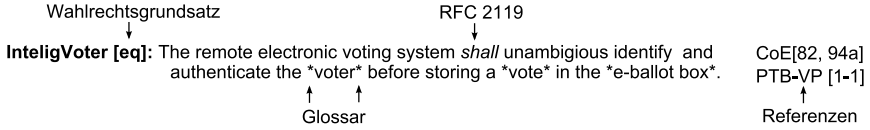

Abbildung 1: Auswahl einer Anforderung aus dem Katalog; mit Syntax/Semantik-Erklärung

3 Evaluierungsverfahren

Die entwickelten Anforderungen an die Sicherheit, Funktionalität und Vertrauenswürdigkeit wurden anschließend in ein standardisiertes Evaluierungsverfahren eingebettet, welches das zugrunde liegende Vertrauensmodell berücksichtigt und die Prüftiefe festlegt. Das Vertrauensmodell umfasst drei Aspekte: die Angreifermächtigkeit, Annahmen an die Einsatzumgebung (z.B., dass bestimmten Komponenten vertraut wird, wie beispielsweise der Integrität des Wählerverzeichnisses) und die Annahme, dass bestimmte Komponenten nicht kooperieren (beispielsweise weil sie unterschiedliche Interessen haben). Die Prüftiefe kann auch als Maß der Vertrauenswürdigkeit in die Systemevaluation bezeichnet werden, denn umso tiefer die Evaluation des Systems ist, umso sicherer kann der Wähler sein, dass die gewünschten Eigenschaften erfüllt werden. Hierbei wird beispielsweise zwischen einem Review des Systemdesigns oder des Quellcodes und einem mathematischen Beweis unterschieden.

Common Criteria Schutzprofil. Es wird vorgeschlagen auf der Common Criteria for Information Technology Security Evaluation (CC) - einem international anerkannten Standard für die Evaluierung von sicherheitskritischen IT-Systemen - aufzusetzen, da dieser flexibel bezüglich unterschiedlichen Vertrauensmodellen und Prüftiefen ist und sich gerade mit den obigen Anforderungen beschäftigt. Dies hat allerdings zur Folge, dass der Schwerpunkt der Evaluierung bei der Internetwahlsoftware liegt und an die Infrastruktur, in der diese Software eingesetzt wird, zwar Anforderungen gestellt werden, diese aber nicht überprüft werden[4]. Daher wurde der entwickelte Anforderungskatalog in die Methodik der Common Criteria übersetzt. Das Ergebnis wird als Schutzprofil im Sinne der CC bezeichnet und trägt den Titel ”Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte” [VV08]. Dieses Schutzprofil wurde inzwischen formal nach den Regeln der Common Criteria durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziert und kann daher bereits jetzt in der Praxis zur Evaluation von Internetwahlsystemen verwendet werden.

Warum aber Basissatz? Da im Schutzprofil das Vertrauensmodell und die Prüftiefe zu definieren sind, kann es nicht ein Schutzprofil geben, welches für Wahlen auf den unterschiedlichen politischen Ebenen geeignet ist: Bundestagswahlen haben einen anderen Schutzbedarf als Vereinswahlen. Daher wurde entschieden, modular vorzugehen: Zunächst wurde ein Basis-Schutzprofil entworfen, welches vorrangig Vereinswahlen adressiert aber gleichzeitig alle Anforderungen bündelt, die an alle anderen Wahlen auch zu stellen sind. Dieses

[4] Um die Infrastruktur zu prüfen, eignet sich beispielsweise der IT-Grundschutzkatalog.

Basis-Schutzprofil ist beliebig erweiterbar und kann letztendlich auch Bundestagswahlen absichern, indem es um die entsprechenden Zusatzanforderungen ergänzt wird. Es definiert das kleinste noch akzeptierbare Vertrauensmodell und die niedrigste noch akzeptierbare Prüftiefe. Hierzu zählt zum Beispiel, dass nicht davon ausgegangen wird, dass ein Angreifer die Ressourcen und die Zeit aufbringt, den PC des Wählers zu manipulieren. Die Prüftiefe wurde auf einer Skala von 1 bis 7 (wobei 1 die schwächste Prüfung ist) auf 2 festgelegt. Hier werden im Wesentlichen eine Evaluation des Systemdesigns sowie verschiedene Systemtests gefordert, nicht aber ein Review des Quellcodes oder gar ein mathematischer Beweis.

Erweiterung des Basis-Schutzprofils hinsichtlich des Vertrauensmodells. Um Erweiterungsmöglichkeiten aber auch deren Konsequenzen aufzuzeigen, wurde das Basis-Vertrauensmodell herabgestuft: Zum einen wurde der Fall diskutiert, dass die Annahme an die Vertrauenswürdigkeit des Wähler PCs nicht gilt, und zum anderen, dass der Angreifer so mächtig ist, dass er in einigen Jahren die heute verwendeten Standard-Verschlüsselungsverfahren brechen kann. Im ersten Fall wird gezeigt, dass ein System, welches mit diesem Angriff umgehen kann, auf Trusted Computing Elemente aufbauen müsste [VASS06] und damit deutlich komplexer wird. Im zweiten Fall besteht das Problem, dass der Angreifer die verschlüsselten Stimmen während der Wahl auf dem Übertragungsweg mitliest, speichert und eben in einigen Jahren entschlüsselt, um das Wahlgeheimnis zu brechen. Es wurde gezeigt, dass nur wenige der bisher existierenden Ansätze Schutz gegen diesen Angriff bieten (z.B. durch den Einsatz eines Zwei-Phasen Modells und blinder Signaturen) [VG08].

Erweiterung des Basis-Schutzprofils hinsichtlich der Prüftiefe. Die im Basisschutzprofil verlangte Prüftiefe ist für Bundestagswahlen nicht angemessen. Da es sich bei dieser Wahl um die wichtigste Wahl handelt, sollte hier entsprechend die intensivste Common Criteria Prüfung (Prüftiefe 7) gefordert werden. Dabei ist zu beachten, dass ab der Prüftiefe 6 der Einsatz von formalen Methoden und ein formales Sicherheitsmodell vorgeschrieben sind, um die Eigenschaften mittels mathematischer Beweise zu zeigen. Formale Methoden sind Techniken zum Modellieren und zur rigorosen Prüfung von IT-Systemen und basieren in der Regel auf mathematischer Logik. Ein formales Sicherheitsmodell existiert für Internetwahlen nicht.

Daher wurde ein erster Schritt unternommen, indem ein formales Teilmodell von Sicherheitsanforderungen mit Methoden der Prädikatenlogik erster Stufe (All- und Existenz-Quantor und mathematische Mengenlehre) entworfen und seine Konsistenz mittels mathematischer Induktion bewiesen wurde. Es handelt sich dabei um ein Zustandsübergangsmodell, das sich aus sicheren Zuständen und erlaubten Zustandsübergängen zusammensetzt. Gezeigt wird, dass sich das System zuverlässig in sicheren Zuständen befinden wird, wenn man annimmt, dass es in einem sicheren Zustand gestartet ist und nur erlaubte Transaktionen durchgeführt werden. Das Teilmodell umfasst folgende Eigenschaften[5]:

- UnauthVotes: $\forall s \in U : voter(s) \in W_{total}$, d.h. in der Urne U befinden sich nur

[5] In [GV08] wurde gezeigt, dass dieses Teilmodell mit dem Wahlgeheimnis vereinbar ist.

Stimmen s von Personen $voter(s)$, die laut Wählerverzeichnis W_{total} wahlberechtigt sind.

- OneVoterOneVote: $\forall s, s' \in U : voter(s) = voter(s') \Rightarrow s = s'$, d.h. die Urne speichert von jedem Wähler nur eine Stimme.
- VoteRight: $\forall x \in W_{total} \setminus W : \exists s \in U : voter(s) = x$, d.h. ein Wähler kann sein Stimmrecht nur dann verlieren (also als 'bereits gewählt' im Wählerverzeichnis markiert werden), wenn seine Stimme erfolgreich in der Urne gespeichert wurde.

Die Vervollständigung dieses Teilmodells auf alle Sicherheitsanforderungen ist Teil eines dieses Jahr startenden DFG Projektes (ModiWa).

k-Resilience-Ausdruck als zusätzliches Prüfkriterium Bei der Umsetzung des Anforderungskatalogs in das Schutzprofil wurde eine Lücke in der Methodik der Common Critieria aufgedeckt: Es besteht keine Möglichkeit das Prinzip der Gewaltenteilung auszudrücken, d.h. dass auch dann kein Angriff erfolgreich durchgeführt werden kann, wenn verschiedene Personengruppen zum Ziel des Angriffs kooperieren. Da das Prinzip der Gewaltenteilung gerade für Wahlen essenziell ist, wird die Einführung eines sogenannten k-resilience-Ausdrucks vorgeschlagen. Dieser stellt ein Maß der Resistenz eines Wahlsystems gegen solche Kooperationsangriffe dar. Es wird empfohlen, neben der Common Criteria Prüfung des Internetwahlsystems auch den k-resilience-Ausdruck berechnen zu lassen. So weiß der Wahlausrichter wem er vertrauen muss bzw. wo er organisatorische Maßnahmen ergreifen sollte, um das Vertrauen zu stärken. Eine solche Maßnahme könnte darin bestehen, alle Administratortätigkeiten am Wahlserver mit einer Videokamera aufzuzeichnen, wie es bei der Wahl in Estland der Fall war.

4 Anwendung des Evaluierungsverfahrens auf Internetwahlsysteme

Das in Kapitel 3 entwickelte Basis-Schutzprofil wurde auf existierende Systeme angewendet. Damit wird zum einen die generelle Anwendbarkeit des Schutzprofils gezeigt und zum anderen die Konformität der Systeme nachgewiesen bzw. widerlegt. Die Prüfung erfolgt auf der Basis der Systembeschreibung. Es wurden folgende Systeme untersucht:

- Das POLYAS System [RJ07], welches seit 2004 bei den Präsidiumswahlen der Gesellschaft für Informatik, seit 2003 bei den Vorstandswahlen der Initiative 21 und 2007 bei der Fachkollegienwahl der Deutschen Forschungsgemeinschaft eingesetzt wurde. Das System arbeitet mit drei Komponenten: Einem Wählerverzeichnis, welches die Stimmberechtigung prüft, einer Urne, welche die Stimmen speichert und einem Validator, der den korrekten Ablauf überprüft. Vereinfacht gesagt wird das Wahlgeheimnis dadurch sichergestellt, dass der Wähler vom Wählerverzeichnis ein zufälliges Wählertoken erhält, mit dem er sich bei der Urne authentifiziert.

- Das Internetwahlsystem aus Estland [Off07], welches 2005 für Kommunalwahlen und 2007 für Nationalratswahlen eingesetzt wurde. Das System arbeitet im Wesentlichen mit zwei Komponenten: Einem Wahlserver, der die verschlüsselten und anschließend vom Wähler signierten Stimmen entgegen nimmt und die Wahlberechtigung prüft, und einer Offline-Auszähleinheit, die die Stimmen entschlüsselt und auszählt. Das Wahlgeheimnis wird hier dadurch sichergestellt, dass die Signaturen von den verschlüsselten Stimmen erst entfernt und die verschlüsselten Stimmen dann durchmischt werden, bevor diese anonymisierten verschlüsselten Stimmen ausgezählt werden.
- Das niederländische RIES System [JV07], welches von 2004 bis 2008 für die dortigen Water Management Wahlen und 2006 für Auslandsbürger bei den Nationalratswahlen eingesetzt wurde: Dieses System arbeitet im Wesentlichen mit einem Wahlserver – einem sogenannten Bulletin Board, auf dem die verschlüsselten Stimmen gespeichert werden. Dieses System bietet dem Wähler die Möglichkeit zu prüfen, ob seine abgegeben Stimme auch gezählt wird - allerdings auf eine Art und Weise, die das Wahlgeheimnis verletzt.

Das Ergebnis dieser Prüfung ist, dass die beiden ersten Systeme nach kleineren Anpassungen positiv evaluiert werden können[6] während das RIES System den Anforderungen hinsichtlich des Wahlgeheimnisses nicht genügt.

Neben der Evaluierung in Anlehnung an die Common Criteria wurde für das POLYAS und das estnische System der k-resilience-Ausdruck bestimmt. Dieser ist für beide Systeme unterschiedlich: Vereinfacht gesagt könnte beim estnischen System der Administrator unbemerkt die Wahl manipulieren, während im POLYAS System die Administratoren von drei Servern entsprechend zusammenarbeiten müssten.

5 Conclusion

Motiviert durch die Vorteile von Internetwahlen einerseits und die fehlenden Evaluierungsverfahren andererseits wurde schrittweise ein standardisierter, umfassender und in sich konsistenter sowie produktunabhängiger Anforderungs- und Evaluierungskatalog für Internetwahlsysteme in Form eines Common Criteria Basis-Schutzprofils entwickelt. Dieses Basis-Schutzprofil wurde an einigen Stellen exemplarisch erweitert, um einerseits die Erweiterbarkeit aufzuzeigen, andererseits aber auch die Konsequenzen für die technische Umsetzung im Internetwahlsystem zu verdeutlichen. Im Rahmen der Entwicklung des Schutzprofils wurde eine Schwachstelle der Common Criteria aufgedeckt und vorgeschlagen, diese durch die Berechnung des k-resilience-Ausdrucks zu schließen. Beide Evaluierungsansätze - das Basis-Schutzprofil und die Berechnung des k-resilience Ausdrucks - wurden auf drei existierende Internetwahlsysteme ¡angewendet, um die Anwendbarkeit der Evaluierungstechniken zu zeigen und die Sicherheit dieser bereits eingesetzten Systeme zu evaluieren.

[6] Der Hersteller Micromata ist derzeit dabei, sein POLYAS System nach dem Basis-Schutzprofil zu evaluieren.

Insgesamt liefert die Arbeit für die derzeitig sehr lebendige wissenschaftliche und politische Auseinandersetzung um Internetwahlen eine wissenschaftlich-rationale Basis, um die Sicherheit von Systemen zu beschreiben, zu prüfen und zu bewerten und trägt dadurch zur Versachlichung der Auseinandersetzung bei.

Literatur

[AV07] Ammar Alkassar und Melanie Volkamer, Hrsg. *E-Voting and Identity – First International Conference, VOTE-ID 2007*, Jgg. 4896 of *LNCS*, Berlin/Heidelberg, 2007. Springer-Verlag.

[Cou04] Council of Europe. Legal, Operational and Technical Standards for E-Voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe and explanatory memorandum. Council of Europe Publishing, 2004.

[GV08] Rüdiger Grimm und Melanie Volkamer. Development of a Formal IT-Security Model for Remote Electronic Voting Systems. In *Proceedings, Electronic Voting 2008*. GI Lecture Notes on Informatics, 8 2008.

[HMR04] Volker Hartmann, Nils Meissner und Dieter Richter. Online Voting Systems for Non-parliamentary Elections - Catalogue of Requirements. Laborbericht PTB-8.5-2004-1, Physikalisch-Technische Bundesanstalt Braunscheig und Berlin (Fachbereich Metrologische Informationstechnik), 2004.

[HPR92] Volker Hammer, Ulrich Pordesch und Alexander Ronagel. KORA – eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlgen fr Informations- und Kommunikationssysteme. Arbeitspapier 100, provet, 1992.

[JV07] Hugo Jonker und Melanie Volkamer. Compliance of RIES to the Proposed e-Voting Protection Profile. In Alkassar und Volkamer [AV07], Seiten 50–61.

[Off07] Office for Democratic Institutions and Human Rights. Republic of Estonia - Parliamentary Elections - 4 March 2007 - OSCE/ODIHR Election Assessment Mission Report. Bericht, Organization for Security and Co-operation in Europe, 2007.

[RJ07] Kai Reinhard und Wolfgang Jung. Compliance of POLYAS with the BSI Protection Profile - Basic Requirements for Remote Electronic Voting Systems. In Alkassar und Volkamer [AV07], Seiten 62–75.

[Sto96] Neil R. Storey. *Safety Critical Computer Systems*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1996.

[VASS06] Melanie Volkamer, Ammar Alkassar, Ahmad-Reza Sadeghi und Stefan Schultz. Enabling the Application of Open Systems like PCs for Online Voting. In *Proceedings of the Frontiers in Electronic Elections – FEE '06*, 2006.

[Ver99] Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland: Bundeswahlgeräteverordnung (BWahlGV), 1999.

[VG08] Melanie Volkamer und Rüdiger Grimm. Trust Model for Remote Electronic Voting. In *Electronic Government - EGOV '08 - 6th International EGOV Conference - Proceedings of Ongoing Research, Project Contributions and Workshops*, Jgg. 27 of *Schriftenreihe Informatik*, Seiten 197–204, Linz, 2008. Universitätsverlag Rudolf Trauner.

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

[VV08] Melanie Volkamer und Roland Vogt. Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte. Commom Criteria Protection Profile BSI-CC PP-0037, `http://www.bsi.de/zertifiz/zert/reporte/pp0037b.pdf`, 2008.

Melanie Volkamer wurde 1980 in München geboren. Im Jahr 1999 nahm sie das Studium zur Diplom-Informatikerin an der Universität des Saarlandes auf. Ihre Diplomarbeit schrieb sie am Bundestamt für Sicherheit in der Informationstechnik. Nach Abschluss ihres Studiums im Jahr 2004 begann Melanie Volkamer als Wissenschaftliche Mitarbeiterin am Deutschen Forschungszentrum für Künstliche Intelligenz. Dort verfasst sie unter anderem zwei Common Criteria Schutzprofile im Kontext von elektronischen Wahlen. Nach ihrem DAAD Aufenthalt an der TU Eindhoven wechselte Melanie Volkamer im Jahr 2007 an die Universität Passau als Geschäftsführerin des Instituts für IT-Sicherheit und Sicherheitsrecht. In dieser Zeit war sie als OSZE Wahlbeobachterin bei den Nationalratswahlen in Estland und als Sachverständige beim Bundesverfassungsgericht im Verfahren über die Wahlprüfungsbeschwerde. Um sich wieder mehr der Forschung widmend zu können, wechselte sie nach Abschluss ihrer Promotion an die TU Darmstadt.