Overview Online-Wahlen

Melanie Volkamer[1] Robert Krimmer[2]

[1]Deutsches Forschungszentrum für Künstliche Intelligenz, GmbH (Saarbrücken)
volkamer@dfki.de

[2]Wirtschaftsuniversität Wien, Department für Informationswirtschaft
robert@krimmer.at

Zusammenfassung

Wissenschaftliche Arbeiten im Bereich Online-Wahlen werden seit den frühen 80er Jahren erstellt. Seit dem Einzug des Internets wurden auch zahlreiche Online-Wahlen durchgeführt. Dies geschah in Deutschland vor allem im Umfeld von Vereinen. Beispielsweise hat die Gesellschaft für Informatik (GI) 2004 ihre Präsidiumswahlen [GI04] und 2005 sowohl Präsidiums- als auch Vorstandswahlen online durchgeführt [GI05]. Auch die Initiative D21 hat ihre Vorstandswahlen 2003 [D2103] und auch 2005 [D2105] elektronisch abgewickelt. In Österreich stehen online Hochschulwahlen im Vordergrund. So fanden 2003 und 2004 zwei Pilotprojekte an der Wirtschaftsuniversität Wien statt [PKKU03, PKKU04]. In der Schweiz werden die weitgediegensten Bestrebungen auf nationalstaatlicher Ebene im Rahmen von drei Pilotprojekten in Genf, Neuenburg und Zürich [Brau04] unternommen. Dies alles soll zum Anlass genommen werden, die inzwischen entstandenen Arbeiten und Systeme aufzubereiten und so einen Überblick über den State of the Art im Bereich Online-Wahlen zu geben. Der Artikel gibt einen Einblick in die Thematik und die aktuellen Diskussionen. Der Schwerpunkt liegt auf den technischen Anforderungen und entsprechenden Lösungsansätzen, die in den verschiedenen Systemen zum Einsatz kamen.

Grundlagen

Wir nutzen das Internet für Homebanking, zum Einkaufen und zum Buchen von Reisen, warum nicht auch zum Wählen? Auf den ersten Blick scheint die Online-Wahl nur eine weitere Applikation zu sein: man meldet sich an dem System an, authentifiziert sich und gibt seine Stimme über eine verschlüsselte Verbindung ab. So einfach ist dies aber leider nicht, denn für Wahlen gelten strenge Regelungen, die eingehalten werden müssen und aus denen entsprechende Anforderungen an die Online-Wahl als solche und vor allem an ein Online-Wahlsystem abzuleiten sind. Darüber hinaus handelt sich es bei Online-Wahlen um ein interdisziplinäres Thema [PrKr04]: Zur Einführung von Online-Wahlen verlangt es die Zusammenarbeit von Politikern, die die Entscheidung für die Einführung treffen, von Juristen, die die Wahlgesetze ändern und die Anforderungen definieren, sowie die Techniker, die das System implementieren, die Soziologen, die sich mit Fragen der Wählerakzeptanz und des Wählervertrauens beschäftigen und zuletzt der Wahlorganisatoren, die beispielsweise das elektronische Wählerverzeichnis erstellen. Einige Aufgaben lassen sich nicht alleine einer Disziplin

zuordnen. Beispielsweise müssen Juristen für die Gesetzesänderungen Anforderungen an die Wahlsoftware stellen. Für die Formulierung der technischen Anforderungen fehlt ihnen das entsprechende Know-how. Auch das Schaffen von Vertrauen und Akzeptanz steht nicht für sich alleine, sondern hängt von der gesamten Projektplanung ab, in wie weit die Öffentlichkeit informiert wird oder gar die Möglichkeit hat, bei der Planung mitzusprechen. Gerade die rechtlichen Rahmenbedingungen, technischen Lösungsansätzen und gesellschaftlichen Handlungskonzepte erfordert die Zusammenarbeit aller betroffenen Disziplinen.

Um die Zusammenhänge besser verstehen zu können, wird im Folgenden die Aufgabe jeder Disziplin besprochen. Zunächst gibt der Artikel aus juristischer Sicht einen Einblick in die Thematik. Dazu werden die verschiedenen Formen der Online-Wahl in Abhängigkeit vom Ort der Stimmabgabe klassifiziert und die Rechtsgrundlagen der jeweiligen Form diskutiert. Im Anschluss beschäftigt sich der Beitrag dann mit den technischen Anforderungen an Online-Wahlen aus juristischer und technischer Sicht. Anschließend wird das Thema aus technischer Sicht genauer beleuchtet. Hierzu werden die bekanntesten drei technischen Protokollansätze vorgestellt und bezüglich der Einhaltung der zuvor definierten Anforderungen untersucht. Den Abschluss bildet eine Diskussion der offenen Probleme und der Zukunft von Online-Wahlen in Deutschland, Österreich und der Schweiz.

Wahlformen und Rechtsgrundlagen

Unter Online-Wahlen verstehen wir alle Wahlformen, bei denen die Stimme online abgegeben wird. In Abhängigkeit vom Ort der Stimmabgabe werden folgende Formen unterschieden:

1.) Muss der Wähler wie bisher ins Wahllokal gehen, um dort an einem Terminal seine Stimme abzugeben, spricht man von einer „*Online-Wahl im Wahllokal*“.

2.) Werden an öffentlich zugängigen Plätzen wie Büchereien und Supermärkten Online-Wahlterminals aufgestellt, so spricht man von einer „*Kiosk Online-Wahl*“.

3.) Die interessanteste Form der Online-Wahl ist die „*remote Online-Wahl*“. Hierbei gibt der Wähler seine Stimme an einem beliebigen Ort von einem beliebigen elektronischen Endgerät ab. Dieser Beitrag konzentriert sich im Folgenden auf diese Form der Online-Wahl.

Nicht zu verwechseln sind diese Formen mit den elektronischen stand-alone Wahlgeräten, die beispielsweise in Deutschland, den Niederlanden und in den USA eingesetzt werden. Hier erfolgt die Stimmabgabe zwar elektronisch, aber die Stimmen werden lokal gespeichert und auch an jedem Gerät separat ausgezählt.

Der Hintergrund dieser Aufteilung ist in den rechtlichen Regelungen für Wahlen zu sehen. Die remote Online-Wahl zählt genau wie die Briefwahl juristisch zur Distanzwahl. Hier kann der Wahlveranstalter nicht mehr sicherstellen, dass der Wähler seine Stimme unbeobachtet und unbeeinflusst abgeben kann und auch tatsächlich abgibt. Die remote Online-Wahl kann unter diesem Aspekt nur in Verbindung mit den entsprechenden Auflagen für Briefwahlen eingesetzt werden. Bei parlamentarischen Wahlen ist der Einsatz der Briefwahl in der Schweiz voraussetzungslos, in Deutschland nur in Ausnahmefällen und in Österreich nur im Ausland zugelassen. Entsprechendes würde dann für die Online-Wahlen gelten. Oftmals existieren auch Wahlen, die als reine Briefwahl durchgeführt werden (beispielsweise die Sozialwahlen oder Wahlen in großen Vereinen in Deutschland). Offensichtlich eignen sich aus juristischer Sicht Wahlen, die bisher als reine Distanzwahlen durchgeführt werden, besser für

die Einführung von Online-Wahlen als andere. Hier sind die Distanzwahlprobleme als solche nicht mehr zu diskutieren, da man sie bereits mit der Zulassung der Briefwahl akzeptiert hat.

Von einer flächendeckenden gesetzlichen Zulässigkeit von Online-Wahlen sind wir noch weit entfernt. Wie die Regelungen im Einzelnen aussehen, ist abhängig vom Land, in dem die Wahl durchgeführt werden soll. Während in Deutschland ausschließlich elektronische standalone Wahlgeräte und Online-Wahlen nur in Einzelfällen (beispielsweise bei Wahlen in der Gesellschaft für Informatik e.V..) zulässig sind, sind in Österreich Online-Wahlen im Rahmen der Hochschülerschafts- und der Wirtschaftskammerwahlen [Stan05, WKWO01] zugelassen. In der Schweiz sind Online-Wahlen nur zeitlich begrenzt im Rahmen des Vote électronique Projekts bis 2006 möglich [Bra04].

Die Systemanforderungen und die Zuständigkeiten für Prüfung und Zulassung eines Online-Wahlsystems sind in den unterschiedlichen Ländern und Einsatzgebieten verschieden. Beispielsweise fordert die Gesellschaft für Informatik e.V., dass die Online-Wahl genauso sicher sein muss wie die Briefwahl. Es werden aber keine Aussagen über die Prüfung gemacht. Die schweizerische Verordnung über die politischen Rechte legt eine Reihe von Sicherheitsanforderungen in [Sch03] fest und fordert für die Zulassung, dass „die Erfüllung der Sicherheitsanforderungen und die Funktionalität des elektronischen Abstimmungssystems [..] von einer unabhängigen, von der Bundeskanzlei anerkannten externen Stelle bestätigt“ werden muss“ [Sch03]. In Österreich sehen die Regelungen im Rahmen des Hochschülerschafts- und Wirtschaftskammergesetzes den Einsatz von Online-Wahlen nur dann vor, wenn das entsprechend einzusetzende System eine Überprüfung entsprechend Signaturgesetz erfüllt hat [Krim02].

Auch wenn die Formulierungen unterschiedlich sind, so ist doch das Gleiche gemeint, denn unabhängig vom Land oder der konkreten Wahl werden die Anforderungen aus den fünf Wahlrechtsgrundsätzen – einer allgemeinen, gleichen, freien, geheimen und unmittelbaren Wahl – abgeleitet.

Systemanforderungen

Es existieren weltweit eine Reihe von Überlegungen, Anforderungen an ein Online-Wahlsystem zu definieren (für eine Übersicht vgl. [VoMe05]). Die bekanntesten und detailliertesten Zusammenstellungen von Anforderungen an Online-Wahlsysteme sind der Anforderungskatalog für „Online-Wahlen für nicht-parlamentarische Wahlen“ der Physikalisch-Technischen Bundesanstalt PTB [HaMR04] und die Empfehlungen des Europarates [CoE04]. Der Anforderungskatalog der PTB wurde im Rahmen des vom Bundesministerium für Wirtschaft und Arbeit (BMWA) geförderten Projektes „Entwicklung von Konzepten für die Prüfung und Zertifizierung von Online-Wahlsystemen“ erarbeitet und beschäftigt sich ausschließlich mit Online-Wahlen im Wahllokal. Der Europarat hat 2004 unter dem Namen „Legal, operational and technical standards for e-voting – Rec(2004) 11“ seine Empfehlungen bezüglich (remote) Online-Wahlen veröffentlicht. Diese beziehen sich auf alle Formen von Online-Wahlen. Diese sind sehr allgemein gehalten, so dass jedes Land diese Empfehlung noch entsprechend seiner eigenen Gesetzeslage instanziieren muss.

Ein Abgleich der einzelnen Anforderungskataloge zeigt, dass sich die Anforderungen in drei Kategorien unterteilen lassen: die *funktionalen* und *sicherheitstechnischen Anforderungen* an das Online-Wahlsystem sowie die *organisatorischen Anforderungen* an die Wahlvorbereitung und -durchführung. Nach [LGT+03] sind funktionale Systemanforderungen solche, die für je-

de Wahldurchführung anders definiert werden können und durch deren Änderungen die Wahlrechtsgrundsätze unbeeinflusst bleiben. Diese Anforderungen legen die Wahlverantwortlichen fest. Funktionale Anforderungen betreffen beispielsweise die Darstellung und Ausgestaltung des Stimmzettels (Auf welche Art und Weise wird die ungültige Stimmabgabe ermöglicht? Soll der Wähler darauf hingewiesen werden, wenn er eine ungültige Stimme abgibt? Aber auch Punkte wie Mehrfachstimmabgabe, d.h. dass der Wähler seine Stimme revidieren kann, fallen unter funktionale Anforderungen). Eine weitere funktionale Anforderung an ein Online-Wahlsystem ergibt sich aus der Forderung nach einer allgemeinen Wahl, die verlangt, dass niemand von der Wahl ausgeschlossen wird. Da nicht angenommen werden kann, dass jeder Wähler die Möglichkeit und/oder die Fähigkeit hat, seine Stimme am PC abzugeben, muss zunächst immer noch eine Alternative angeboten werden. Unabhängig davon ist die Frage zu klären, welche Rechner unterstützt werden sollen. In der Regel wird es ausgeschlossen sein, für alle möglichen PCs, Web-Browser und Internetverbindungen das remote Wahlsystem auf Funktionsfähigkeit zu testen.

Die organisatorischen Anforderungen betreffen die Aufgaben, die nicht von dem System erledigt werden können. Hier wird beispielsweise die Erstellung und Einsicht in ein elektronisches Wählerverzeichnis geregelt, aber auch die Informierung der Wähler und die Verteilung von Wählerauthentifizierungsmerkmalen – falls erforderlich. Während die funktionalen und organisatorischen Anforderungen solche sind, die die Wahlverantwortlichen individuell festlegen können, werden unter den Sicherheitsanforderungen alle Anforderungen zusammengefasst, die jedes Online-Wahlsystem erfüllen muss, damit es die Wahlrechtsgrundsätze einhält. Vereinfacht zählen folgende Anforderungen zu den Sicherheitsanforderungen eines Online-Wahlsystems:

1. Zu keinem Zeitpunkt darf es möglich sein, eine Zuordnung von einem Wähler und seiner abgegebenen Stimme herzustellen. Darüber hinaus darf das System dem Wähler nicht die Möglichkeit geben, seine Stimme gegenüber Dritten zu beweisen (*Anonymität* – (zeitlich unbegrenzte)[1] *geheime* Wahl).
2. Eine zuverlässige und „eindeutige“ Identifizierung der Wähler muss sichergestellt werden, damit zum einen kein berechtigter Wähler von der Wahl ausgeschlossen wird und zum anderen, damit jeder Wähler nur einmal wählen kann (*Authentifizierung – allgemeine* und *gleiche* Wahl).
3. Es darf an keiner Stelle – weder bei (der Stimmabgabe am Endgerät, bei) der Übertragung noch bei der Speicherung möglich sein, Stimmen unbemerkt zu verändern, zu löschen oder hinzuzufügen (*Integrität – allgemeine, freie* und *gleiche* Wahl).
4. Das Ergebnis muss korrekt ausgezählt werden, insbesondere müssen alle abgegebenen Stimmen auch in die Ergebnisberechnung einfließen (*Korrektheit – allgemeine, freie* und *gleiche* Wahl)
5. Das Online-Wahlsystem muss sicherstellen, dass bei sämtlichen Ausfällen der Server oder eines Endgeräts, weder Stimmen verloren gehen, noch verändert oder doppelt gespeichert werden. Außerdem darf bei einem Wiederanlauf die Anonymität nicht verletzt werden (*Robustheit – allgemeine, freie* und *gleiche* Wahl).

[1] Die Angaben in Klammern sind von den Autoren als sinnvoll empfundene Ergänzungen zu den Anforderungen aus den bekannten Katalogen.

6. Die Berechnung von Zwischenergebnissen muss ausgeschlossen werden *(Zugriffskontrolle – gleiche* Wahl).

In den meisten Anforderungskatalogen fehlt allerdings ein wichtiger Aspekt: die *Rand- und Rahmenbedingungen,* unter denen ein Online-Wahlsystem die definierten Anforderungen erfüllen muss. Daher kann derzeit gar nicht entschieden werden, ob ein System konform mit den Anforderungen ist oder nicht. Die Entscheidung des Evaluators hängt von den Rand- und Rahmenbedingungen ab, die er sich definiert. Es reicht also nicht, diese Sicherheitsanforderungen in den Gesetzen zu verankern, sondern es muss definiert werden, unter welchen Bedingungen das Online-Wahlsystem diese Sicherheitsanforderungen erfüllen muss. Hierzu zählt die Definition von Anforderungen an die (IT-)Einsatzumgebung und eine Bedrohungsanalyse[2] sowie die Definition des Bedrohungspotenzials[3] bzw. der Angreifermächtigkeit. Es muss also aufgeteilt werden in Bedrohungen, die das System abwehren muss und Annahmen, die als gegeben angenommen werden und wofür keine Sicherheitsmechanismen vorhanden sein müssen. Beispielsweise kann entweder angenommen werden, dass das Endgerät des Wählers nicht manipuliert ist, oder man formuliert eine Bedrohung, in der der Angreifer durch die Manipulation des Endgerätes versucht, einen der Wahlrechtsgrundsätze zu verletzen. Nur im zweiten Fall muss das Online-Wahlsystem sicherstellen, dass eine Manipulation des Endgerätes keine Auswirkungen hat, während im ersten Fall der Wähler dafür zuständig ist.

Diese Erkenntnis legt die Formulierung von Anforderungen in Form eines Common Criteria Schutzprofils nahe, da hier vor der Definition der Sicherheitsanforderungen die Annahmen und Bedrohungen sowie die Angreifermächtigkeit festgelegt wird. Dieser Ansatz würde weitere Vorteile wie eine Vereinheitlichung und eine internationale Anerkennung der Anforderungen und Produktzertifikate implizieren. Darüber hinaus ist hier das Vorgehen zur Prüfung bekannt und hat sich bewährt. Zu klären ist an dieser Stelle die Frage, welche Evaluierungsstufe für welche Art der Wahl (ob Vereinswahlen oder parlamentarische Wahlen) gefordert werden muss.

Systemansätze

Es haben sich drei Formen herauskristallisiert, nach denen sich Online-Wahlsysteme sortieren lassen:

- nach dem eingesetzten Authentifizierungsmechanismus (basierend auf dem Geheimnis-, Besitz- oder Eigenschaftsprinzip),
- nach der Client-Lösung (je nachdem, ob die Kommunikation mit den Servern über einen herkömmlichen Browser oder eine spezielle Client-Software erfolgt)
- oder nach dem Wahlprotokoll (hier wird nach dem Anonymisierungsmechanismus unterschieden).

[2] Die Bedrohungsanalyse legt die bedrohenden Personen, die Angriffszenarien und die bedrohten Werte/Daten fest.

[3] Zur Ermittlung des Bedrohungspotenzials beschränkt man sich auf reale Bedrohungen und definiert das Profil des Angreifers (Know-how, Gelegenheit, technische Ausstattung, Motivation).

Die jeweiligen Ansätze unterscheiden sich bezüglich ihrer Sicherheit und damit in der Erfüllung der Sicherheitsanforderungen, aber auch in Bezug auf Benutzerfreundlichkeit und der entstehenden Kosten. In Abhängigkeit vom Einsatzgebiet müssen hier jeweils die Sicherheit und die Kosten gegeneinander aufgewogen werden. Zu beachten ist dabei, dass nicht jede Kombination bezüglich Varianten der drei Klassen möglich ist.

Eingesetzte Wählerauthentifizierung

Bei der Wählerauthentifizierung kann zwischen den üblichen Authentifizierungsmerkmalen (Geheimnis, Besitz und Eigenschaft) unterschieden werden. Die erste Variante ist die einfachste und benutzerfreundlichste. Hierbei erhält der Wähler vor der Wahl ein so genanntes Wahlpasswort (bzw. auch Wahl-PIN oder Wahl-TAN genannt). Dies kann beispielsweise auf dem Postweg geschehen. Um ein Ausspähen des Geheimnisses bei der Übertragung zum Wähler auszuschließen, benötigt der Wähler bei der Anmeldung am Wahlsystem neben dem Wahlpasswort weitere persönliche Daten. Bei den GI-Wahlen war beispielsweise die Eingabe der GI-Mitgliedsnummer verlangt. Problematisch ist dieser Ansatz bzgl. der Einhaltung der Authentifizierungsanforderung (2), da das Passwort gegebenenfalls auch zusammen mit den anderen persönlichen Daten erraten oder weitergegeben werden kann, beispielsweise zwecks Stimmenkaufs. Die Stärke der Authentifizierung ist dabei vergleichbar mit der Briefwahl, da auch hier nicht ausgeschlossen werden kann, dass jemand Drittes die Unterlagen aus dem Postfach entfernt oder ein Wähler die Unterlagen unterschreibt und dann weitergibt. Allerdings ist hier der Aufwand größer, da die Übertragung nicht elektronisch erfolgen kann.

Eine Erhöhung der Sicherheit kann an dieser Stelle durch den Einsatz von elektronischen Karten als Authentifizierungsmerkmal erhöht werden. Diese lassen sich nur unter erheblichem Aufwand im großen Maße weitergeben, insbesondere dann, wenn die Karten auch in anderen Bereichen zur Authentifizierung eingesetzt werden. Eine Kombination von Besitz und Geheimnis in Form von qualifizierten digitalen Signaturkarten käme einer Abbildung des Authentifizierungsmechanismus der Briefwahl am nächsten. Allerdings sind diese Karten in der Praxis noch nicht vorhanden, so dass für den Einsatz bei Wahlen derzeit enorme Kosten entstehen würden. Einen Lösungsansatz könnten die österreichischen und deutschen Konzepte der Bürgerkarte bieten, wo jeweils die eindeutige Identifizierung der Bürger mittels einer Signaturkarte angedacht (D) bzw. teilweise schon umgesetzt (A) sind. Die nächste Stufe ist die Authentifizierung basierend auf biometrischen Eigenschaften. Hierbei wird eine Sicherheitsstufe für die Authentifizierungsanforderung (2) erreicht, die vergleichbar mit der im Wahllokal ist. Allerdings gilt hier genau wie bei den Signaturkarten, dass derzeit noch eine flächendeckende Verbreitung fehlt und daher der Einsatz bei Wahlen mit sehr hohen Kosten verbunden wäre.

Client-Lösung

Der Wähler muss zur Stimmabgabe mit dem Endgerät (in der Regel ein PC) auf die Server zugreifen können, um seine Stimme dort abzugeben. Hierzu werden zwei verschiedene Ansätze *Web-Browser-Lösung, Rich-Client-Lösung* - unterschieden. Die Web-Browser-Lösung ist aus Wählersicht die benutzerfreundlichere und aus Sicht der Wahlveranstalter die kostengünstigere Variante. Der Wähler braucht sich keine spezielle Wahlsoftware zu installieren, sondern ruft die entsprechende Web-Seite des Wahlservers über seinen Web-Browser

auf. Auf diese Weise kann recht einfach sichergestellt werden, dass möglichst viele Wähler ihre Stimme problemlos online abgeben können. Mit diesem Argument wurden auch die GI-Wahlen auf Basis einer Web-Browser-Lösung durchgeführt. Die gesamte Funktionalität liegt dabei bei dem oder den Wahlserver/n. Der Client dient nur zur Eingabe und Versendung der Authentisierungsangaben und des Stimmzettels. Die Kommunikation basiert auf den vorhandenen Verschlüsselungsprotokollen wie SSL. Durch die fehlende Client-Funktionalität können nur wenige und i. a. nur die schwächeren Wahlprotokolle im Zusammenhang mit der Web-Browser-Lösung eingesetzt werden. Die Einbeziehung aller Protokolle und damit eine höhere Sicherheit ermöglicht die Rich-Client-Lösung in Form einer eigenen Client-Wahlsoftware. Der Preis für die höhere Sicherheit ist der Mehraufwand beim Wähler durch die Installation der Wahlsoftware einerseits, aber auch die Schwierigkeit, eine Software zu implementieren, die auf möglichst allen Rechnern und Betriebssystemen installiert werden kann (um die Allgemeinheit der Wahl gewährleisten zu können)[4]. Außerdem muss sichergestellt werden, dass die Wähler eine authentische Wahlsoftware verwenden.

Bei beiden Client-Ansätzen darf die Vertrauenswürdigkeit der Endgeräte nicht außer Acht gelassen werden. Das Endgerät ist bei remote Online-Wahlen das schwächste Glied in der Sicherheitskette (vgl. [Rub01] und [StHo02]) und ihm muss daher besondere Beachtung zukommen. Bösartige unentdeckte Software auf dem Endgerät kann automatisch beliebigen Schaden anrichten und damit die meisten Sicherheitsanforderungen (1-4) verletzen. Beispielsweise könnte ein Trojaner die Zugangsdaten bei der Eingabe abfangen und an den Angreifer schicken, damit dieser die Stimme abgeben kann (2). Die Malware könnte darüber hinaus auch die Stimme vor dem Versenden verändern (3,4), im Klartext an den Angreifer verschicken (1) oder die erfolgreiche Stimmabgabe dem Wähler nur vortäuschen (3,4). Die GI [GI05] begegnet diesem Problem mit der Verteilung von Handreichungen, wie der Wähler seinen PC absichern kann. Wird die Vertrauenswürdigkeit des Endgerätes nicht in Form von Annahmen in die Hände des Wählers gelegt, muss das Online-Wahlsystem die Vertrauenswürdigkeit des Endgerätes sicherstellen. Hierzu existieren eine Reihe von Ansätzen: angefangen mit einfachen Checks durch einen Rich-Client, bevor die eigentliche Wahlapplikation gestartet wird, bis hin zu Trusted Computing [SenVo06]. Einen ähnlichen Vorschlag macht Otten in [Otte01], in dem er ein eigenes Wahlbetriebssystem vorschlägt. Die Idee ist dabei, eine Knoppix-ähnliche CD zu verteilen, die der Wähler booten und über die er dann seine Stimme abgibt. Inzwischen ist Knoppix so gut entwickelt, dass sie auf einem Großteil der PCs gebootet werden kann, so dass eine Abwandlung als Wahlbetriebssystem denkbar wäre. Problematisch ist hierbei der Internetzugang, diesen erkennt die CD nicht automatisch, sondern muss vom User eingerichtet werden. Zudem würden aus Komplexitätsgründen enorme Kosten für eine Prüfung entstehen. Auch in diesem Fall ist damit eine Erhöhung der Sicherheit nur zu Lasten der Benutzerfreundlichkeit und durch erhöhte Kosten zu erreichen. Einen anderen Vorschlag bezüglich der Vertraulichkeit schlagen Fischer und Zuser in [FisZu05] vor: dem Client soll erst gar nicht das Wissen über den Inhalt des Stimmzettels geben werden. Damit kann er die Stimme nicht gezielt verändern, und auch ein Verschicken im Klartext ist nicht mehr möglich.

[4] Hierbei sind insbesondere Probleme mit der Installation der Software entscheidend, weil der Wähler hierzu seine Systemkonfiguration kennen muss. Für weitere Schwierigkeiten siehe [PKKU03; PKKU04]

Das Wahlprotokoll

Die Herstellung der Anonymität bei gleichzeitiger eindeutiger Identifizierung und Authentifizierung des Wahlberechtigten gilt in den Kreisen von Kryptographen als die Königsdisziplin [CESG02]. Dies erklärt auch die große Anzahl an technischen Lösungsvorschlägen in Form von Wahlprotokollen. Hierzu werden die bekannten krytographischen Algorithmen und Mechanismen wie Signaturen, blinde Signaturen, MIX-Kaskaden, Homomorphe Verschlüsselung, Zufallszahlen usw. eingesetzt. Für die Einteilung der verwendeten Anonymitätsverfahren existieren in Bezug auf Online-Wahlen bereits umfangreiche Untersuchungen, die die vorhandenen Wahlprotokolle in Protokollfamilien untergliedern. Neben [HoMi95, LGT+03 und Smit05] hat Schlifni die differenziertesten Einteilungen [Schl00, S: 130] mit acht verschiedenen Varianten getroffen, von denen in der Praxis nur die folgenden drei Kategorien eingesetzt werden, die bezüglich der Durchsetzung der Sicherheitsanforderungen an ein Wahlprotokoll (1und 3) untersucht werden:

1) Systeme mit vorgelagerter Wähleridentifizierung: Hier existiert die klassische Zweiteilung. Erst wird der Wähler authentifiziert und in einem zweiten Schritt erfolgt die anonyme Stimmabgabe über ein aus Schritt 1 erhaltenes anonymes Token. Eine einfache Ausprägung dieser Protokollklasse zeichnet sich durch eine organisatorische Anonymisierung im Vorfeld der Wahl aus. Hierbei werden anonyme Token vor der Wahl erzeugt und nur an Wahlberechtigte verteilt. Es muss organisatorisch sichergestellt werden, dass bei der Erstellung und Verteilung der anonymen Token keine Zuordnung zwischen Wähler und dem erhaltenen Geheimnis möglich ist. Bei der eigentlichen Stimmabgabe ist dann kein Anonymisierungsmechanismus mehr erforderlich, und die Stimme wird zusammen mit diesem Token in verschlüsselter Form an die Wahlserver zur Auszählung geschickt. Dort werden nach Wahlende alle Stimmen, die an ein gültiges Geheimnis gebunden sind, ausgezählt. Dabei wird sichergestellt, dass zu jedem Geheimnis nur eine Stimme gezählt wird. Auf diese Art und Weise wird selbst gegen einen Angreifer, der die Kommunikation mitliest und in Zukunft in der Lage sein wird die Nachrichten zu entschlüsseln die geheime Stimme sichergestellt (1). Allerdings kann ein Wähler durch die Bekanntgabe seines anonymen Tokens gegenüber einem mitlesenden Angreifer seine Stimme beweisen. Um ausschließen zu können, dass die Stimme bei der Übertragung verändert oder gelöscht wird (3), quittiert der Wahlserver dem Wähler den Erhalt der Stimme. Ein Hinzufügen von Stimmen auf dem Kommunikationsweg kann ausgeschlossen werden, wenn das anonyme Token groß genug gewählt ist, so dass ein Angreifer durch Ausprobieren seine Stimme nicht mit einem gültigen Token an den Wahlserver schicken kann. Problematisch ist bei dieser Form die aus praktischen Gründen manchmal erforderliche Entfernung von Wahlberechtigten aus dem Wählerverzeichnis während der Wahl. Dies ist nicht möglich, da die Geheimnisse anonym auf dem Urnenserver gespeichert sind. Bei einer zweiten Variante erfolgt auch der erste Schritt elektronisch. Der Wähler authentifiziert sich bei einem Wahlserver (Wählerverzeichnis) entweder mittels persönlicher Daten und einem zugeschickten personalisierten geheimen Wahltoken oder mit seiner persönlichen digitalen Signatur. Wenn dies erfolgreich war, erhält der Wähler ein anonymes Berechtigungstoken, mit dem er im zweiten Schritt seine Stimme ohne die Angabe von persönlichen Identifikationsdaten abgeben kann. Damit ist der Wähler zwar gegenüber dem zweiten Server anonym, aber ein Angreifer, der beide Nachrichtensequenzen kennt, kann diese sehr wohl zuordnen, so dass die zeitlich unbegrenzte geheime Wahl nicht sichergestellt werden kann (1). Bezüglich des Hinzufügens,

Löschens und Veränderns von Stimmen auf dem Kommunikationsweg (3) gilt analog zu dem vorherigen Ansatz, dass dies mit entsprechenden Mechanismen sichergestellt werden kann. Neben dem Einsatz bei der GI-Wahl [GI04, GI05] wird diese Variante auch bei den Projekten in Genf und Zürich [Brau04] verwendet.

2) Systeme mit verdeckter Auswertung: Bei Systemen mit verdeckter Auswertung handelt es sich um Verfahren, bei denen die einzelne Stimme nicht im Klartext bekannt wird, ihr Besitzer aber sehr wohl bekannt ist. Die Anonymität wird dadurch gesichert, dass nur die Summe über alle Stimmen in entschlüsselter Form vorliegt. Durch diesen Verfahrensablauf gelten diese Online-Wahlsysteme als besonders nachvollziehbar. Insbesondere erfüllen sie eine teilweise zusätzliche geforderte Eigenschaft: Verifikation durch den Wähler. Er kann feststellen, ob seine Stimme gezählt wurde und das Ergebnis korrekt berechnet wurde. Daher werden diese Verfahren bei Wahlen eingesetzt, bei denen die Stimmabgabe über mehrere Kanäle möglich ist, d.h. entweder die klassische Mehrfachstimmabgabe auf elektronischem Wege oder die Möglichkeit nach Abgabe der elektronischen Stimmen, diese durch eine Papierstimme zu „überschreiben“. Diese Eigenschaft wird in der Praxis auf zwei Arten realisiert – entweder durch den Einsatz von Hardware Security Modulen (HSM) oder durch homomorphe Kryptographie. HSM werden zur Wahrung der Anonymität in der Weise eingesetzt, dass die verschlüsselten Stimmen im HSM decodiert und ausgezählt werden. Dabei können Stimmen nicht einzeln, sondern nur in ihrer Summe ausgelesen werden. Solch ein System kam bei den estnischen Lokalwahlen [Maat04] im Herbst 2005 zum Einsatz. Die homomorphen Verfahren beruhen auf homomorpher Verschlüsselung der Stimmzettel. Dann braucht man zur Wahlauswertung nur die verschlüsselten Stimmen miteinander zu verknüpfen (in der Regel zu multiplizieren), denn dies (ggf. das Produkt) entspricht der verschlüsselten Summe der einzelnen Stimmzettel. Durch diese Eigenschaft können die Stimmen gezählt werden, ohne eine einzelne Stimme zu kennen. Das bekannteste Protokoll wurde von Schoenmakers [Scho99] vorgestellt und war Basis des EU CyberVote Projekts. Die Sicherstellung der geheimen Wahl beruht bei diesen Verfahren darauf, dass die Auszählung tatsächlich verdeckt erfolgt. Dies erfordert zusätzlich organisatorische Maßnahmen für die Geheimhaltung der entsprechenden Schlüssel. Beide Verfahren können zwar die Anforderung 3 durch geeignete Mechanismen erfüllen, aber gegenüber einem Angreifer, der die Protokollnachrichten auf dem Netz kennt, nicht die zeitlich unbegrenzte geheime Wahl sicherstellen (1).

3) Systeme mit Pseudonymisierung: Diese Online-Wahlprotokolle beruhen auf Chaum’s blinden elektronischen Signaturen [Chau81]. Diese Technologie wird auf zwei Varianten eingesetzt: Entweder lässt sich der Wähler den selbst geblindeten Stimmzettel vom Wählerverzeichnis signierten, um die entblindete Stimme dann anonym an die Urne schicken zu können (wie in [FuOO93]) oder das blind signierte Dokument des Wählers an das Wählerverzeichnis ist ein anonymes Pseudonym (wie in [PrMü02]), welches vom Wählerverzeichnis signiert wird. Das entblindete und vom Wählerverzeichnis signierte Token erlaubt dem Wähler dann seine Stimme anonym bei der Urne abzugeben. Dies sichert die Anonymität gegenüber den Komponenten maximal ab, allerdings scheitert auch dieses Protokoll bei der Erfüllung einer zeitlich unbegrenzten geheimen Wahl (1), wenn der Angreifer in der Lage ist, die Kommunikation mitzulesen. Dafür kann aber ausgeschlossen werden, dass Stimmen bei der Übertragung unbemerkt gelöscht, verändert oder hinzugefügt werden (3).

In Abhängigkeit von der Angreifermächtigkeit hat sich gezeigt, dass die beschriebenen Protokolle bezüglich der Anonymisierung noch nicht sicher genug sind. Es empfiehlt sich ggf. weitere Mechanismen wie Mehrfachstimmabgabe oder MIX-Kaskaden zu implementieren.

Zu den Protokollen, die bisher in der Praxis noch nicht eingesetzt wurden zählen u. a. solche ohne vertrauenswürdige Instanz [BeYu86] beispielsweise in Form eines Wahlservers. Der Wähler kann selbst sicherstellen, dass eine Ergebnismanipulation aufgedeckt wird und die Anonymität gesichert ist. Der Preis hierfür ist ein enormes Nachrichtenaufkommen, so dass solche Protokolle nur in sehr kleinen Wählergruppen effizient eingesetzt werden können.

Ausblick

Verschiedene Sammlungen wissenschaftlicher Arbeiten aus allen Bereichen (politisch, gesetzlich, technisch, organisatorisch) zeigen, dass Online-Wahlen in den einzelnen Disziplinen gut untersucht sind. Was aber die Frage aufkommen lässt, warum es noch nicht zur flächendeckenden Einsetzung von Online-Wahlsystemen gekommen ist, warum der deutsche Online-Wahlen-Pionier Prof. Otten sein Vorhaben „zur Europawahl 2004 […] ein rechtskräftiges Wahlverfahren über das Internet anbieten zu können“ [Roet99] nicht umsetzen konnte bzw. warum die Bundestagswahlen 2005 in Deutschland nicht wie von der Initiative D21 [Init02] gefordert online durchgeführt wurden?

Ein Grund liegt in der sicherlich sehr komplexen und vielschichtigen Materie, die insbesondere eine interdisziplinäre Behandlung notwendig macht. Denn technische Probleme wie eine fehlende Infrastruktur (Vorhandensein von Signaturkarten) sind nicht ohne die politische Unterstützung zu lösen. Doch Politiker haben eigene Ziele zu verfolgen, und hier muss die Einführung von alternativen Wahlformen nicht unbedingt zur Zielerreichung dienlich sein (das findet seine Bestätigung u. a. auch im „Mittelsmann-Paradoxon“ [MaKr05]). Auch die zu lösenden rechtlichen Probleme mit der Vereinbarkeit von elektronischen Wahlen mit dem Grundgesetz führt nicht zuletzt zu fortlaufenden Zweifeln an der Reife der neuen Technologie für den Einsatz in althergebrachten Prozessen.

Bei der Einführung von technischen Neuerungen hat sich bis jetzt immer die stufenweise Erprobung und Evaluierung dieser neuen Technologien bezahlt gemacht. Im Falle von elektronischen Wahlen muss zudem noch die singuläre Betrachtungsweise der Technikfolgen abgelegt und zu einer vernetzten und interdisziplinären Lösungsstrategie gewechselt werden. – Nur so kann in unmittelbarer Zukunft der nächsten 5 Jahren außerhalb von reinen Vereinswahlen z.B. bei den Sozialwahlen ein erfolgreicher Einsatz dieses Modernisierungsschubes der Demokratie möglich sein.

Literatur

[BeYu86] Benaloh, J. D., Yung, M.: Distributing the power of a government to enhance the privacy of voters. S. 52–62,1986.

[Brau04] N. Braun (2004): E-Voting: Switzerland's Projects and their Legal Framework, Proceedings of the ESF TED Workshop on Electronic Voting in Europe, Schloss Hofen/Bregenz 43-52.

[Chau81] D. Chaum (1981): Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, Communications of the ACM, 24(2), S. 84-88

[CoE04] Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommundation Rec(2004)11 and explanatory memorandum, Council of Europe, Strassbourg, pp. 87.

[D2103] Initiative D21 (2003): Die D21-Vorstandswahl, In: http://www.initiatived21.de/themen/egovernment_anwendungen/doc/37_1071075505.pdf, abgerufen am 2005-10-18

[D2105] Initiative D21 (2005): Die D21-Vorstandswahl, In http://www.initiatived21.de /presse/presseinformationen/pages/show.prl?params=recent%3D1%26type% 3D 10%26all%3Dall%26keyword%3D%26laufzeit%3D&id=13102&currPage=1, abgerufen am 2005-10-18

[FisZu05] G. Fischer, W. Zuser (2005): Increasing election secrecy: The vote scrambling algorithm. Technical Report der Technischen Universität Wien

[FuOO93] A. Fujioka, T. Okamoto, K., Ohta (1993): A Practical Secret Voting Scheme for Large Scale Elections. In: Advances in Cryptology – AUSCRYPT92. Springer-Verlag, Berlin 1993. 244–251.

[GESG02] Communications and Electronic Security Group (CESG) (2002): E-Voting Security Study. Issue 1.2, 57 Seiten.

[GI04] Heise Online (2004): Gesellschaft für Informatik wählte Präsidium erstmals online, In: http://www.heise.de/newsticker/meldung/54204, abgerufen am 10-10-2005

[GI05] Gesellschaft für Informatik e.V.: Wahlen (2005), In http://www.gi-ev.de/wahlen2005/, abgerufen am 10-10-2005

[HaMR04] V. Hartmann, N. Meißner, D. Richter (2004):Online Voting Systems for Non-parliamentary Elections: Catalogue of Requirements, Berlin: PTB Bericht 8.5-2004-1, 54

[HoMi95] P. Horster, M. Michels (1995): Der Vertrauensaspekt in elektronischen Wahlen, in: Horster, P. (ed.), Trust Center, Vieweg, Braunschweig 180-189.

[Krim02] Krimmer, R. (2002): e-Voting.at - Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen, Diplomarbeit, WU Wien.

[LGT+03] C. Lambrinoudakis, D. A. Gritzalis, V. Tsoumas, M. Karyda, S. Ikonomopoulos: Secure Electronic Voting: The Current Landscape, in: Secure Electronic Voting, Kluwer Academic Publishers, Boston + Dordrecht, 101-122 (2003)

[Maat04] Maaten, E. (2004): Towards Remote E-Voting: Estonian Case, Proceedings of the ESF TED Workshop on Electronic Voting in Europe, Schloss Hofen/Bregenz, S. 83-90.

[MaKr05] Mahrer, H., Krimmer, R. (2005): Towards the enhancement of e-democracy: identifying the notion of the?middleman paradox?, Information Systems Journal, Vol. 15, Nr. 1, pp. 27-42.

[LGT+03] C. Lambrinoudakis, D. A. Gritzalis, V. Tsoumas, M. Karyda, S. Ikonomopoulos: Secure Electronic Voting: The Current Landscape, in Secure Electronic Voting, Kluwer Academic Publishers, Boston + Dordrecht, 101-122 (2003)

[Otte01] D. Otten (2001): Wählen wie im Schlaraffenland? Erfahrungen der Forschungsgruppe Internetwahlen mit dem Internet als Wahlmedium, in: Holznagel, B., Grünwald, A., and Hanßman, A. (eds.), Elektronische Demokratie: Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis, Verlag C.H. Beck, München 73-85.

[PKKU03] A. Prosser, R. Krimmer, R. Kofler, M.K. Unger (2003): Die erste Internet-Wahl Österreichs. Ein Erfahrungsbericht von E-Voting.at. Working Paper Nr. 04/2003 des Instituts für Informationsverarbeitung und –wirtschaft der Wirtschaftsuniversität Wien.

[PKKU04] A. Prosser, R. Krimmer, R. Kofler, M.K. Unger (2004): e-Voting Wahltest zur Bundespräsidentschaftswahl. Working Paper Nr. 01/2004des Instituts für Informationsverarbeitung und –wirtschaft der Wirtschaftsuniversität Wien, 2004.

[PrKr04] A. Prosser, R. Krimmer (2004): Dimensions of Electronic Voting. In: Electronic Voting in Europe, S.21-28.

[PrMu02] A. Prosser, R. Müller-Török: E-Democracy (2002): Eine neue Qualität im demokratischen Entscheidungsprozess, Wirtschaftsinformatik, Vol. 44, Nr. 6, S. 545-556.

[Roet99] Rötzer, F. (1999): Wahlen im Internet, http://www.heise.de/newsticker/meldung/5216 abgerufen am 12-09-2005.

[Rub01] A D Rubin (2001): Security Considerations for Remote Electronic Voting over the Internet, http://avirubin.com/e-voting.security.pdf, abgerufen am 10-10-2005

[Sch03] Der Schweizerische Bundesrat (2003) Verordnung über die politischen Rechte, gestützt auf Artikel 91 Absatz 1 des Bundesgesetzes über die politischen Rechte (Gesetz, BPR); Abschnitt 61: Pilotversuche mit elektronischer Stimmabgabe

[Schl00] M. Schlifni (2000): Electronic Voting Systems and Electronic Democracy: Participatory E-politics for a New Wave of Democracy, Dissertation, Technische Universität, Wien.

[Scho99] B. Schoenmakers (1999): A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting, Advances in Cryptology - Crypto99, (Vol. 1666) Springer-Verlag 148-164.

[SenVo06] O. Senf, M. Volkamer (2006): Application of Trusted Computing for eVoting, Technical Report

[Smit05] W. D. Smith (2005): Cryptography meets Voting, http://www.math.temple.edu/~wds/homepage/cryptovot.pdf, abgerufen am 07-07-2005.

[Stan05] Stangl, S. (2005): Österreichisches Hochschulrecht: Hochschülerschaftsgesetz 1998, Hochschülerschaftswahlordnung 2005, (Vol. 15), Bundesministerium für Bildung, Wissenschaft und Kultur, Vienna, pp. 155.

[StHo04] J. R. Stuart, V. Hooper (2004): Security Considerations for Remote Internet Voting, http://www.lgnz.co.nz/library/files/store_007/Security_Considerations_for_Remote_Internet_Voting.pdf, abgerufen am 2005-10-21.

[VoMe05] M. Volkamer, N. Meißner (2005): Anforderungskataloge für Online-Wahlen, http://www.dfki.de/fuse/AnforderungskatalogCC.ppt, abgerufen am 10-10-2005

[WKWO01] Wirtschaftskammer-Wahlordnung (WKWO), BGBL. I Nr. 153/2001.