Elektronische Wahlen in geschlossenen Benutzergruppen

Bernd Fix <bernd@wauland.de>, Vortrag auf der COSIN 2011

Gleich am Anfang mal eine Warnung: Dies wird ein interaktiver Vortrag – mitdenken und mitreden sind nicht nur zulässig, sondern ausdrücklich gewünscht.

Ich werde im folgenden immer in der männlichen Form sprechen, wenn es um Wähler, Wahlberechtigter u.s.w. geht; natürlich sind auch die weiblichen Formen damit eingeschlossen. In der Schweiz ist das gerade in Bezug auf Wahlen ja nicht ungewohnt, denn das Frauenwahlrecht gibt es erst seit 40 Jahren...

Warum ist dies ein Ketzervortrag?

Ganz klar: Weil man als **CCC'ler** doch weiss, dass elektronisches Wählen grundsätzlich böse ist und niemals sicher und anonym sein kann, das hat der CCC doch schon immer gesagt...

Ich halte es allerdings mit der **Hackerethik**, in der steht: „**Misstraue Autoritäten**“ und ich finde, das sollte auch und vor allem bei **selbst-erschaffenen Autoritäten** wie dem CCC gelten – auch wenn einige das gerne unter der Rubrik „Gedankenverbrechen“ einordnen möchten...

Klassischer Ablauf einer Wahl

Bei einer klassischen Wahl geben die **Wahlberechtigten** ihre Stimme (Votum) ab; die Stimmen fliessen in den **Wahlprozess** ein, den wir hier mal als „Black Box“ darstellen wollen. Aus dieser „Black Box“ fliesst nach Ende der Wahl ein **kumuliertes Gesamtergebnis** heraus; hier als Tortengrafik dargestellt.

Die Frage, wie gewählt werden sollte, hängt jetzt wesentlich davon ab, ob wir (als Wähler) dem **Wahlergebnis vertrauen** können. In allen Diskussionen, die auch im CCC und Umfeld zu dieser Frage geführt wurden, wird das Vertrauen in das Ergebnis immer aus dem Vertrauen in den Wahlprozess abgeleitet. Dazu darf der Wahlprozess natürlich keine „Black Box“ mehr sein; man muss die **inneren Abläufe** verstehen und bewerten können.

Wann vertrauen wir einem Wahlprozess?

Vertrauen in einen Wahlprozess setzt voraus, dass der Ablauf bestimmte funktionale Anforderungen erfüllt:

Da ist zum einen die **Korrektheit der Auszählung**, die sicherstellen muss, dass jede **abgegebene Stimme** korrekt verbucht ist, dass nur **berechtigte Stimmen** gezählt werden und dass jeder Wahlberechtigte **nur eine Stimme** hat.

Zusätzlich wird auch gerne die nicht-funktionale Anforderung gestellt, dass das **Wahlgeheimnis** gewahrt werden muss, d.h. es darf nicht möglich sein, die Stimme eines Wählers zu ermitteln.

Apropos „Wahlgeheimnis“...

Warum ist vielen Wählern das **Wahlgeheimnis** so wichtig?

Ich habe auch erst an angefangen, über den Sinn (oder Unsinn) des Wahlgeheimnisses nachzudenken, als ich in die Schweiz kam und wohnte. Es war mir in Diskussionen aufgefallen, dass in der Schweiz viele Leute das Wahlgeheimnis als weniger wichtig erachten, als in Deutschland – so zumindest mein Eindruck...

Dann wurde mir klar, das Wahlen in der Schweiz – die ja nun unstrittig sehr viel länger praktiziert werden als in Deutschland – immer sehr offen gehandhabt wurden: Alle Wahlberechtigten haben sich auf der Allmende getroffen und durch Hand-heben ihre Stimme abgegeben; jeder wusste, was der Urs, der Sepp und der Beat von nebenan für eine Wahl-Meinung haben. So etwas wie Wahlgeheimnis war unbekannt, aber es wurden

offensichtlich auch nur wenige totgeschlagen, weil sie anders abgestimmt haben...

Ich glaube, dass ein **Wahlgeheimnis** vor allem in den Gesellschaften für wichtig erachtet wird, in denen Menschen auf Grund ihrer politischen Einstellung benachteiligt, verfolgt, eingesperrt, gefoltert oder sogar ermordet wurden oder werden – wie eben zum Beispiel in Deutschland. Damit ist – böse ausgedrückt – das Wahlgeheimnis eher der Ausdruck einer fehlenden **Maturität** einer Gesellschaft als ein zu erhaltendes demokratisches Gut...

Warum basiert das Vertrauen in ein Wahlergebnis auf dem Vertrauen in den Wahlprozess?

Nach dem kurzen Abschweifen über das Wahlgeheimnis noch mal zurück zu der Frage: Warum basiert das **Vertrauen in das Wahlergebnis** auf dem Vertrauen in den Wahlprozess?

Dazu noch mal das **Schema** der klassischen Wahl von vorhin...

Antwort: kein Wähler kann das Ergebnis der Wahl direkt **kontrollieren**, d.h. er hat keine Möglichkeit, zu prüfen, ob seine Stimme korrekt verbucht ist, weil mit dem Einwerfen des Wahlzettels in die Urne der Wahlzettel **anonymisiert** ist (Wahlgeheimnis). Zudem ist das Ergebnis kumuliert, ein **Nachzählen** durch jeden Wähler ist unmöglich, weil bei einer Papierwahl völlig unpraktikabel.

Vertrauen in das Ergebnis = Vertrauen in den Wahlprozess

Deshalb gilt beim klassischen **Wahlverfahren**: Vertrauen in das Ergebnis = Vertrauen in den Wahlprozess. Aber schon **Lenin** wusste: Vertrauen ist gut, Kontrolle ist besser!

Was also wäre, wenn jeder das Wahlergebnis **selbst und direkt** vollständig kontrollieren könnte? Dann wäre es eigentlich **egal, wie** das Wahlverfahren aussieht...

Kontrollierbares Wahlergebnis

Klar ist, das in einem solchen Fall das Wahlergebnis nicht mehr nur eine einfache

Tortengraphik sein kann, vielmehr müssen **alle abgegeben Stimmen** einsehbar sein:

Jeder Wähler hat ein – nur ihm bekanntes – Pseudonym, unter dem sein Votum veröffentlicht ist. Nach Ende der Wahl kann er in der Ergebnisliste sein **Votum kontrollieren** (ist meine Stimme korrekt verbucht) und da das alle Wähler können, kann er von der inhaltlichen Korrektheit der gesamten Liste ausgehen.

Da er alle Stimmzettel kennt, kann er auch die Stimmen selbst **zusammenzählen** und so das Endergebnis kontrollieren.

Was ist das Problem bei einer solchen Ergebnisliste?

Kein Wähler kann **entscheiden**, ob alle Einträge der Liste auch wirklich zu berechtigten Wählern gehören und dass jeder Wähler tatsächlich nur ein Votum abgeben konnte.

Kurze Anmerkung: Das Problem würde nicht existieren, wenn das Wahlgeheimnis nicht gewahrt werden müsste: Statt des Pseudonyms wäre der richtige Name des Wählers aufgeführt, der sein Votum per (elektronischer) Unterschrift beglaubigt.

Wie löst man das **Problem**, wenn das Wahlgeheimnis gewahrt werden soll? Das Verfahren muss sicherstellen, dass – wie vorhin schon mal aufgeführt – nur **berechtigte** Wähler ihre Stimme abgeben können und das jeder Wähler auch **nur eine Stimme** hat.

Die von mir vorgeschlagene Problemlösung verletzt nicht das **Wahlgeheimnis** und basiert auf kryptographischen Verfahren (**PKI**).

Einer der berechtigten Kritikpunkte des CCC an elektronischen Wahlen, die Kryptoverfahren einsetzen, ist die Tatsache, dass es irgendwo immer einen **MasterKey** gibt, mit dessen Kenntnis die Wahl manipuliert werden kann. In dem Verfahren von mir ist das nicht der Fall, weil es keine zentrale Instanz mit einem Generalschlüssel gibt!

Ablauf: Schritt 1 – Veröffentlichung der Wählerlisten

Die Wählergruppe bestehe aus *n* Personen, die – ganz analog zu PGP – jede ihr eigenes, selbsterstelltes RSA-Schlüsselpaar besitzt; tatsächlich können sogar vorhandene

PGP/GnuPG-Schlüsselbunde für das Wahlverfahren genutzt werden.

Es gibt keine zentrale Instanz, die einen Schlüssel einer Person per Zertifikat zuordnet (CA), aber es ist wie bei PGP von definitivem Vorteil, wenn der öffentlichen Schlüssel eines Wählers durch mindestens einen anderes Wahlberechtigten gegengezeichnet sind, so das sich ein „Web Of Trust“ bildet. Sowohl die öffentlichen Schlüssel als auch die gegenseitigen Signierungen der Schlüssel sind dabei öffentlich zugänglich.

In einem **ersten Schritt** veröffentlicht der Wahlausschuss, z.B. der Vorstand eines Vereins, die Wählerliste. In dieser **Liste** sind alle Wahlberechtigten samt ihres öffentlichen Schlüssels aufgelistet und für alle Wähler einsehbar.

Ablauf: Schritt 2 – Ausüben der Wahl

Für die Wahl **erfindet** jeder Wähler für sich ein Kürzel, das nur ihm bekannt ist. Eigentlich ist das Kürzel ein Längsel, weil es eindeutig sein muss – keine zwei Wähler sollten per Zufall das gleiche Kürzel wählen.

Dann erstellt der Wähler sein **Wahlticket**, auf dem sein Kürzel und sein Votum vermerkt sind. Länge der Felder sowie ihr Format sind vorgegeben und sind natürlich vorher vom Wahlausschuss publiziert worden.

Ablauf: Schritt 3 – Verpacken der Wahltickets in Umschläge

Das Wahlticket wird im folgenden als Bithaufen betrachtet, die als „ziemlich lange Zahl“ interpretiert wird. Diese Zahl wird jetzt kryptographisch **eingetütet**, damit ihr Inhalt später von anderen blind signiert werden kann. Der Wähler unterschreibt auf dem Umschlag, so dass der nachfolgende **Blindsignierer** weiss, von vom der Umschlag kommt – ohne zu wissen, was im Umschlag ist.

Übertragen auf die nicht-elektrische Welt kann man sich diesen Vorgang so vorstellen: Ich erstelle meinen Wahlzettel, auf dem ich mein selbst-gewähltes Kürzel und meine Wahlentscheidung schreibe. Dann kopiere ich den diesen Wahlzettel für jeden Wähler auf

der Wählerliste (einschliesslich mich selbst) und tüte jeden kopierten Zettel zusammen mit Kohlepapier (Durchschlagpapier) in einen vorher von mir unterschriebenen Umschlag ein und verklebe ihn. Jetzt schicke ich den Umschlag an jeden Wähler der Liste.

Ablauf: Schritt 4 – Blindsignatur der Umschläge

Jeder Wähler **unterschreibt** jetzt blind alle Umschläge, die für ihn bestimmt sind und schickt sie (an den Absender) zurück. Vorher kontrolliert er natürlich die Unterschrift des Absenders (die in der Wählerliste stehen muss) und kontrolliert, das jeder Absender nur einen Umschlag bei ihm eingereicht hat.

Kurze Randnotiz: Das **kryptographische** Verfahren der Blindsignatur wurde 1983 von David Chaum entwickelt, um elektronische Wahlen abzuhalten, aber dafür bisher nie eingesetzt. Statt dessen bildete das Verfahren die kryptographische Grundlage für eCash...

Abauf: Schritt 5 – Erstellen des Wahlzettels

Der Wähler öffnet die erhaltenen **Umschläge** und entnimmt das unterschriebene Wahlticket. Alle unterschriebenen Wahltickets werden zu einem Wahlzettel zusammen-geheftet und **anonym** an den Wahlausschuss gesendet.

Ablauf: Schritt 6 – Wahlergebnis und Prüfung

Jeder kann jetzt aus den veröffentlichten **Wahlzetteln** die Gültigkeit aller Stimmen kontrollieren, die ja von allen Wählern gleichermassen unterschrieben sein muss. Zudem kann jeder Wähler die korrekte Verbuchung seines eigenen **Votums** kontrollieren.

Ablauf: Schritt 7 – Revoken eines Wahlzettels

Für den Fall, dass der Rechner eines Wählers gepwnd ist und die Erstellung seines Wahltickets manipuliert wurde und er das erst merkt, nachdem die Wahl beendet ist, dann kann er **anonym** seinen Wahlzettel zurückziehen.

Kryptographisch passiert dies durch die Veröffentlichung der Parameter des Generators, nach dem die Zufallszahlen der Blindsignaturen erzeugt wurden. Dies ist nur möglich, wenn es aus einem gegebenen Satz von Zufallszahlen nicht möglich ist, innerhalb vernünftiger Zeit einen validen Satz von Generator-Parametern zu berechnen.