Electronic voting

26. DECUS Symposium
Bonn, 9. April 2003

Dr. Alexandre Wennmacher

Universität zu Köln
<wennmach@geo.Uni-Koeln.DE>

The NetBSD Project
<wennmach@netbsd.org>

Übersicht

- Einführung
- Konventionelle Wahlen
  - Historischer Hintergrund
  - Einsatz von Technologien
  - Gesetzliche Vorgaben
  - konventionell -> e-voting
- Anforderungen an sichere Wahlen
  - Kriterienerfüllung bei konventionellen Wahlen
- e-voting/i-voting
  - Prinzip
  - Beispiele
- Wahlen im NetBSD Projekt
  - Protokoll
  - Statistik
- Ausblick

Einführung

- Freie Wahlen sind wichtigste Errungenschaft der Demokratie
- Wahlen finden in allen Größenordnungen statt:
  - Kommune
  - Bundesland
  - Land (Bundestag, Sozialwahlen)
  - Europa
  - Welt
- Zahl der Wahlberechtigten
  - Verein (30)
  - Europawahlen, US-Präsidentschaftswahlen (300 Mio.)
- Wahlen sind aufwändig
  - Präsenz meist erforderlich
  - Alternative: Briefwahl?
  - teuere Demokratie: Sozialwahlen
    - alle 6 Jahre (nächstes Mal: 2005)
    - 50 Mio. Wahlberechtigte
    - ausschließlich Briefwahl
    - Kosten 1999: 66 Mio. DM

Historischer Hintergrund/Technologien (1)

- Konzept heutiger Wahlen stammt aus Mitte - Ende des 19. Jahrhunderts
  - Anonymisierung durch Verwendung uniformer Wahlzettel
  - Eintragung der Wähler in Wählerliste
  - Auszählung der Stimmen nach der Wahl unter Kontrolle von Wahlhelfern
- Einsatz von Technologien richtet sich nach der technischen Entwicklung
- Wahlen: Herausforderung an IT-Bereich
  - Bundestagswahlen: über 60 Mio. Wahlberechtigten und Wähler
  - Europawahlen: 1999: 289 762 628 Wahlberechtigte
- Einsatz zeitgemäßer (zunehmend IT) Technologien:
  - Wahlinterface
  - Führen der Wählerliste
  - Managen des Wahlprozesses, inkl. Auszählen der Stimmen

Historischer Hintergrund/Technologien (2)

Beispiel Bundestagswahlen:

- Notwendigkeit an einem bestimmten Tag zum Wahllokal zu gehen
- Aufwändige Ausnahme: Briefwahl
  - in den meisten Ländern der EU nicht zugelassen
- Wählerlisten:
  - computerverwaltet, aber ausgedruckt
  - händisches Prüfen der Wählerindentität
  - händisches Austreichen des Wählers
- Stimmenauszählung:
  - bisher meistens händisch
  - versuchsweiser Einsatz elektronischer Wahlgeräte

Gesetzliche Vorgaben

Gesetze, die die Bundestagswahlen in Deutschland regeln:

- Grundgesetz
- Bundeswahlgesetz
- Bundeswahlordnung
- Bundeswahlgeräteverordnung
- Wahlprüfungsgesetz
- Parteiengesetz

Konventionelle Wahlen -> e-voting

- Wahlprozedere akzeptabel in einem hochindustrialisierten Land mit guter Infrastruktur
- Wahlen in Flächenstaaten wie z. B. Russland oder Alaska
- Globalisierung: Wahlen mit weltweit verteilten Wählern
- -> e-voting - "electronic voting"
  - Konsequenter Einsatz von IT-Technologien in allen Bereichen
- -> i-voting - "Internet Voting"
  - Spezialfall von e-voting
  - Wahlprotokoll wird über das Internet abgewickelt

Aber: Kann e-voting/i-voting sicher sein?

Anforderungen an Wahlen

Fujioka et al. (1993) verlangen von sicheren Wahlen folgende Merkmale:

- [Eligibility] Kein unberechtigte Wähler kann an der Wahl teilnehmen.
- [Unreusability] Jeder Wähler kann maximal eine Stimme abgeben.
- [Completeness] Alle abgegebenen gültigen Stimmen werden korrekt gezählt.
- [Verifyability] Niemand kann das Ergebnis der Wahl (unentdeckt) verfälschen.
- [Privacy] Niemand kann herausfinden wie an anderer Wähler gewählt hat.
- [Soundness] Der unehrliche Wähler kann die Wahl nicht gefährden.
- [Fairness] Die Wahl darf nicht beeinflußt werden.

Bei einigen Wahlen kann es weitere Anforderungen geben, z. B. dass Teilnahme veröffentlicht wird.

Kriterienerfüllung bei Bundestagswahlen (1)

- [Eligibility]
  - Prüfen anhand der Personalausweises ob der Wähler in der Wählerliste verzeichnet ist
  - Beim Vorliegen besonderer Gründe (plötzliche Erkrankung) können Wahlunterlagen am Tag der Wahl für einen Dritten in Empfang genommen werden
  - Problem Briefwahl:
    - Wahlberechtigungsprüfung hier nicht möglich
    - Androhung empfindlicher Strafen bei Missbrauch

Kriterienerfüllung bei Bundestagswahlen (2)

- [Unreusability]
  - Ausstreichen des Wählers aus der Wählerliste nach Ausgabe des Wahlzettel.
  - Kein Schutz gegen Stimmenkauf, allerdings kann der Käufer nicht nachprüfen, ober der gekaufte Wähler wirklich wie aufgetragen gewählt hat
  - Problem Briefwahl:
    - Überprüfbarer Stimmenkauf hier möglich

Kriterienerfüllung bei Bundestagswahlen (3)

- [Completeness]
  - kein direkter Schutz
  - Vertrauen der Wähler in den geregelten Ablauf der Wahl durch
    - öffentliche Auszählung (Viel-Augen-Prinzip)
    - freiwillige Wahlhelfer
    - Wahlprüfer
  - Problem: elektronische Wahlgeräte
    - mangelnde Transparenz

Kriterienerfüllung bei Bundestagswahlen (4)

- [Verifyability]
  - nur indirekt:
    - Wähler kann nicht prüfen, ob seine Stimme korrekt berücksichtigt wurde
    - Plausibilitätsprüfung anhand der Wahlprotokolle
    - Problem: Briefwahl

Kriterienerfüllung bei Bundestagswahlen (5)

- [Privacy]
  - Verwendung von uniformen Wahlzetteln im uniformen Umschlag, Wahlkabinen
  - Problem: Briefwahl
    - Geheimhaltung durch den Briefwähler gesetzlich erfordert
  - Problem: elektronische Wahlgeräte

Kriterienerfüllung bei Bundestagswahlen (6)

- [Soundness]
  - Vertrauen der großen Mehrheit der Staatsbürger
  - Viel-Augen-Prinzip (nur in begrenztem Umfang)
  - Einsatz von ehrenamtlichen, nicht-staatlichen Wahlhelfern
  - Gesetzliche Regelung der Wahl
  - Hohe Strafandrohungen bei Missbrauch

Kriterienerfüllung bei Bundestagswahlen (7)

- [Fairness]
  - Gesetzliche Vorgaben, hohe Strafandrohungen
  - ggfs. Schutz der Wahllokale durch die Polizei

Kriterienerfüllung bei Bundestagswahlen (Zusammenfassung)

- Fälschung konventioneller Wahlen stellt eine niedrige Anforderung dar
- Probleme bei der amerikanischen Präsidentschaftswahl 2000 haben gezeigt, dass konventionelle Wahlverfahren auch ohne kriminelle Absichten gefährdet sind
- Konventionelle Wahlen verfügen über keine technischen Einrichtungen, die Wahlvergehen bei Verschwörung, Regierungskriminalität und Terrorismus ausschließen oder nachweisen können.
- Die Sicherheit des konventionellen Wahlsystems basiert auf:
  - Vertrauen im die ethische und politische Integrität der Wahlvorstände
  - Androhung schwerer Strafen bei Wahlfälschung und -mißbrauch
- Besonders kritisch ist die Sicherheit der Briefwahl zu sehen, die in allen Stadien wesentlich anfälliger ist

e-voting

- Wahlen durch den Einsatz moderner elektronischer Kommunikation in allen Bereichen des Wahlverfahrens
- e-voting muß zumindest in dem gleichen Maß die Anforderungen an Wahlen erfüllen wie konventionelle Wahlen
- Das A und O von e-voting ist die Definition eines geeigneten Wahlprotokolls (unter Zuhilfenahme kryptografischer Methoden):
  - Public Key Verschlüsselung
  - digitale Signatur und Hashwert
  - Infrastruktur gesetzlich kontrollierter Trustcenter
  - Smart Card Technologie
  - blinde Beglaubigungssysteme für anonyme Botschaften
  - "Anonyme Kanäle" zur Lösung der "Traffic Analysis Problems".
- Die Methodenvielfalt ist groß! Tiefergehende Hintergrundinformationen in "Applied Cryptography" von Bruce Schneier.

Beispiele für e-voting

- Wahl zum Studentenparlament an der Universität Osnabrück am 2. 2. 2000
  - Modellprojekt des "Forschungsgruppe Internetwahlen"
- Landesamt für Datenverarbeitung und Statistik Land Brandenburg, Juni 2000
  - Personalvertretung des Landesamtes für Datenverarbeitung und Statistik Brandenburg (LDS BB)
    - Bedingt Internetzugang mit Chipkartenlesetechnik am Arbeitsplatz
    - Ansonsten Wahl in öffentlichen Wahlräumen online
- Jugendgemeinderatswahl Esslingen, Juli 2001
  - europaweit die erste papierlose, signaturkarten-gestützte Wahl zu einem öffentlichen Gremium statt, die allen juristischen Anforderungen genügte.
- Gremienwahl der Universität Bremerhaven, Oktober 2001
  - Wahl der Fachbereichsräte und des Akademische Senat
  - Zugang zum Online-Wahlsystem erfolgte mittels marktüblicher Signaturkarten
- Wahlen im NetBSD Projekt, August/September 2002
  - Abstimmung der Mitglieder über den vom Nomination Committee vorgeschlagenen "Board of Directors"

Das NetBSD Projekt

- Eines der 3 Open-Source Projekte zur Weiterentwicklung des BSD-Betriebsystems
  - NetBSD, FreeBSD, OpenBSD
  - wurde am 23. März 2003 10 Jahre alt
- Schwerpunkte und Zielsetzung
  - Architektonische Sauberkeit
  - Portierbarkeit
  - Interoperabilität
  - BSD Lizenz
- ca. 200 aktive Entwickler, weltweit verteilt
- Reorganisation
  - legitimierte Autoritäten
  - Steuerbefreiung nach IRC 501(c)3 in den USA
  - Bylaws
  - Nomination Committee (siehe RFC 2727) schlägt Board of Directors vor
  - Wahlberechtigte Mitglieder stimmen ab (ja/nein), 51 % Mehrheit erforderlich
  - Wahlleiter: A. Wennmacher

Die Wahlen im NetBSD Projekt

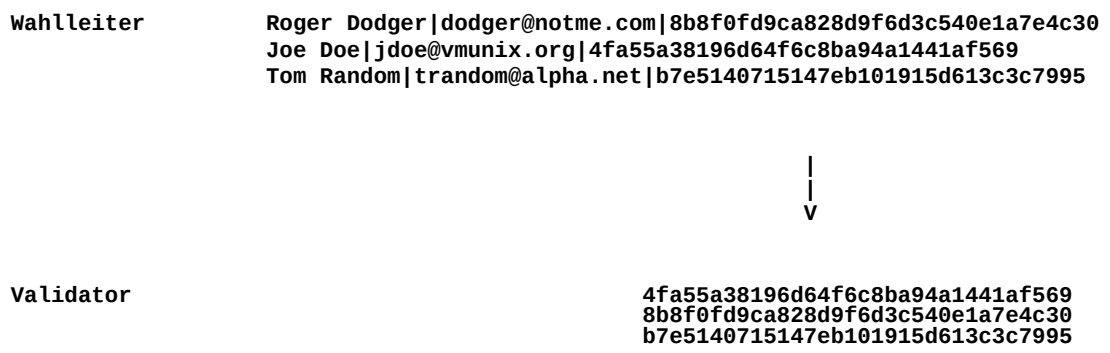
- i-voting wegen weltweiter Verteilung der Mitglieder erforderlich
- Netzzugang bei allen Mitgliedern gegeben
- Sicheres i-voting angestrebt (Erfüllung der Fujioka-Kriterien)
- "Open Protocol" Lösung: keine Verwendung spezieller Wahl-Software, sondern nur:
  - e-mail
  - /dev/random
  - md5
  - PGP/GPG
  - anonymous remailers
- Publikation der detaillierten Wahlprozedur vor Beginn der Wahl

Protokoll (1)

- Der Wahlleiter erstellt und publiziert die vorläufige Liste der Wahlberechtigten.
- Nach Ablauf einer Einspruchsfrist wird die endgültige Liste der Wahlberechtigten und die Zahl der Wahlberechtigten bekanntgegeben.
- Ein Validator wird mit Hilfe eines öffentlich überprüfbaren Zufallsverfahrens (siehe RFC 2777) aus einer Gruppe von Freiwilligen ausgewählt.

Protokoll (2)

- Der Wahlleiter generiert für jeden Wähler einen eindeutigen Wählerschlüssel.
- Der Wahlleiter schickt die Wählerschlüssel (nur diese) an den Validator.
- Der Validator prüft und bestätigt den Wahlberechtigten, dass er soviele verschiedene Wählerschlüssel erhalten hat, wie es zugelassene Wähler gibt.



Protokoll (3)

- Der Wahlleiter schickt jedem Wahlberechtigten seinen Wählerschlüssel per e-mail.

```
Wahlleiter     Roger Dodger|dodger@notme.com|8b8f0fd9ca828d9f6d3c540e1a7e4c30

                                                        |
                                                        |
                                                        V

Roger Dodger                                  8b8f0fd9ca828d9f6d3c540e1a7e4c30
```

Protokoll (4)

- Die Wähler schicken ihr Votum an den Validator.
- Die Wähler können ihr Votum
  - mit Hilfe von Anonymen Remailern anonymisieren
  - mit dem PGP-Schlüssel des Validators verschlüsseln
- Votum besteht aus: (Stimme, Wählerschlüssel, Prüfschlüssel)

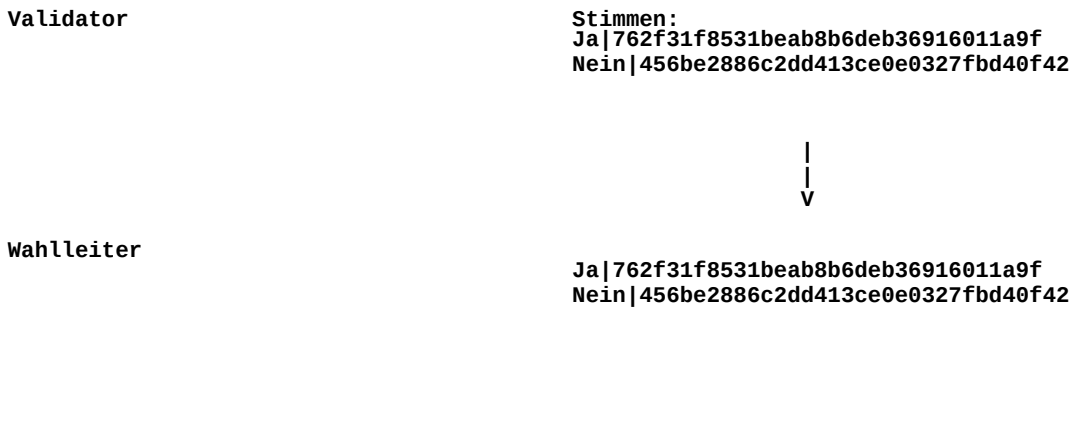
```
Roger Dodger                          Stimme: Ja
                             Wählerschlüssel: 8b8f0fd9ca828d9f6d3c540e1a7e4c30
                               Prüfschlüssel: 762f31f8531beab8b6deb36916011a9f

                                                        |
                                                        |
                                                        V

Validator                             Stimme: Ja
                             Wählerschlüssel: 8b8f0fd9ca828d9f6d3c540e1a7e4c30
                               Prüfschlüssel: 762f31f8531beab8b6deb36916011a9f
```

Protokoll (5a)

- Nach dem Ablauf der Wahlperiode schickt der Validator die empfangenen Wählerschlüssel an den Wahlleiter.

Protokoll (5b)

- Außerdem schickt er dem Wahlleiter separat (nicht den Wählerschlüsseln zuordenbar) die abgegebenen Stimmen zusammen mit den dazugehörigen Prüfschlüsseln.



Protokoll (5c)

- Aus der Liste der empfangenen Wählerschlüssel erzeugt der Wahlleiter die Liste der Wähler. Außerdem zählt der Wahlleiter die Stimmen aus und publiziert das vorläufige Wahlergebnis, zusammen mit den empfangenen Stimmen und Prüfschlüsseln.

```
Wahlleiter publiziert:

Wähler:                         Roger Dodger
                                Joe Doe

Stimmen:                        Ja|762f31f8531beab8b6deb36916011a9f
                                Nein|456be2886c2dd413ce0e0327fbd40f42
```

Protokoll (6)

- Nach der Publikation der vorläufigen Wahlergebnisses kann jeder Wähler anhand des nur ihm bekannten Prüfschlüssels verifizieren, ob seine Stimme auch richtig berücksichtigt wurde.
- Die Wahlberechtigen haben 2 Tage Zeit gegen die Stimmzählung zu protestieren.
  - Wähler können Korrekturen verlangen

Protokoll (7)

- Das endgültige Wahlergebnis wird vom Wahlleiter bekanntgegeben. Die Wahl ist nicht mehr anfechtbar.

Statistik

- Wahlbeteiligung 68 % (124/182)
  - 124 ja
  - 2 nein
  - 0 ungültig

- Wählerverhalten

digital signiert, verschlüsselt	**2**	
digital signiert, Klartext	**4**	**6**
pseudonym, verschlüsselt	**5**	
pseudonym, Klartext	**106**	**111**
anonym, verschlüsselt	**3**	
anonym, Klartext	**4**	**7**

  - nur ca. 6 % der Wähler wählten anonym

Anekdote

- Rätsel: 2 identische(!) Prüfschlüssel empfangen:

  d41d8cd98f00b204e9800998ecf8427e

- Lösung:

In der Anleitung zur Wahl wurde zur Erzeugung des Prüfschlüssels folgender Vorschlag gemacht:

```
[...] The suggested way to create your confirmation code is to use the following command:

 % dd if=/dev/random bs=128 count=1 | md5

Paste the resulting 32 character random string into the template.
```

- Weitere auffällige Prüfschlüssel:
  - 31415926535897932384626433832795
  - three_blind_mice_see_how_they_run
  - <include your confirmation code

Ausblick

- Gewähltes Protokoll war dem Zweck angemessen
  - Erfüllt Fujioka-Kriterien "ziemlich gut"
    - Protokoll empfindlich auf Konspiration Wahlleiter <-> Validator
    - Wählerschlüssel sollten verschlüsselt verschickt werden
- Schema übertragbar auf Wahlen mit vielen Wählern?
  - Problem: DoS-Attacken
  - Problem: Skalierbarkeit
    - Registrierung von PGP-Schlüsseln
- Zertifizierung von Wahl-Software
- Problem: allgemeine Akzeptanz von e-voting/i-voting
  - Größtmögliche Transparenz des Systems
  - Open-Protocol Lösungen
  - Open-Source Lösungen
- Erste i-voting Bundestagswahl wird noch auf sich warten lassen

Literatur

- A. Fujioka, T. Okamoto, K. Ohta, "A Practical Secret Voting Scheme for large Scale Elections", Advances in Cryptology, AUSCRYPT ’92, 1993
- B. Schneier, "Applied Cryptography", John Wiley & Sons, New York, 1996
- A. Wennmacher, http://daily.daemonnews.org/view_story.php3?story_id=3186
- http://lorrie.cranor.org/voting
- http://www.i-vote.de

Ende

Fragen?