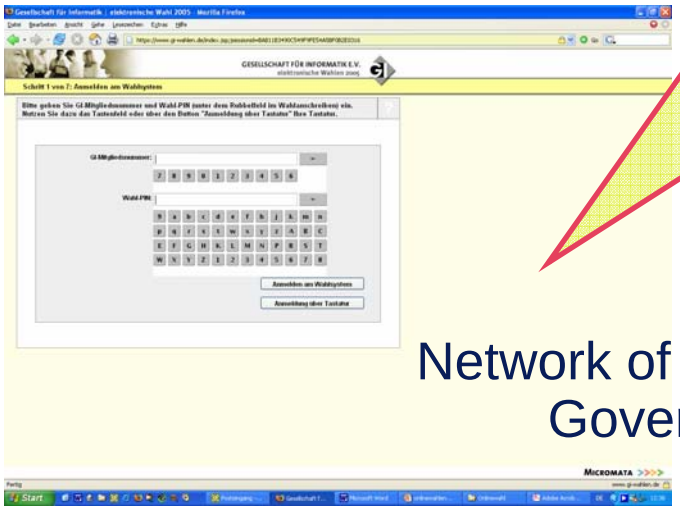
IT-Risk Management und E-Voting



Network of Informatics Research in Governmental Business

eGov Day in Koblenz
31 Januar 2006

Prof. Dr. R. Grimm

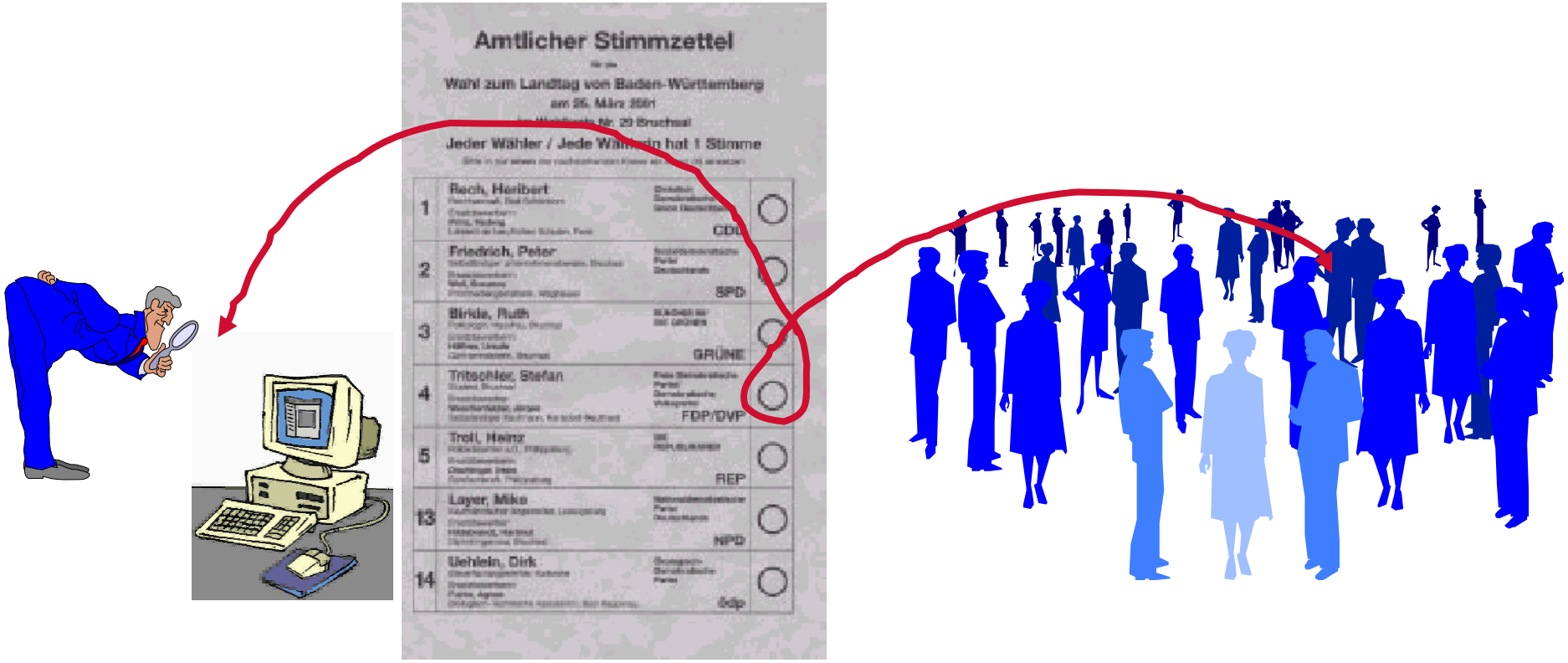
Institut für Wirtschafts- und Verwaltungsinformatik
Universität Koblenz

Inhaltsübersicht

1. **Das Sicherheitsdilemma von Wahlen**
2. IT-Sicherheit
3. Die Werte der demokratischen Wahl
4. Wahlformen
5. Anforderungskatalog
6. GI-Wahlen 2004 und 2005

Dilemma elektronischer Wahlen

Authentisch versus *anonym*



Auch wenn Nutzer in Anwendungen unsichtbar sind...

sie hinterlassen Spuren im Netz:

- IP-Adressen
- Domain Name System
- Log-Files in Routers und Servers
- Kommunikationsprofile
  - HTTP Referer
  - Cookies
- A-posteriori De-anonymisierung von Profilen
- MIX Netze sind teuer (und lösen auch nicht alles)

Auch wenn Nutzer an User-Ids gewöhnt sind...

diese sind unzuverlässig:

- IP-Adressen wechseln
- Email-Adressen sind frei wähl- und fälschbar
- Digitale Signaturen sind teuer und schwer handhabbar
- PINs und TANs praktikable Zwischenlösung
- Wie bindet man TANs/Public Keys/Pseudonyme zuverlässig an Personen?
- Vorbild Homebanking?

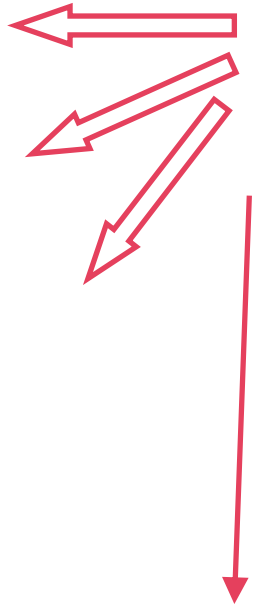
4 Parteien

1. Wahlbüro
   - Können Wähler identifizieren
   - Zertifizieren berechtigte Wähler
2. Wähler
   - Werden authentifiziert
   - Füllen Stimmzettel aus
   - Geben Stimmzettel ab
3. Urne
   - Sammelt Stimmen
4. Zähler
   - Lesen und zählen
   - Veröffentlichen Ergebnis

4 Wahlphasen

Ziel: numerische Auswertung der abgegebenen Stimmen

1. Autorisierung der stimmberechtigten Wähler
   - Antragsteller identifizieren
   - Berechtigte Wähler zertifizieren
2. Stimmabgabe
   - Stimmzettel ausfüllen
3. Stimmsammlung
   - Stimmzettel abgeben
   - Stimmen in Urne sammeln
4. Auszählen
   - Lesen und zählen
   - Ergebnis veröffentlichen



Integrität

Anonymität?

Inhaltsübersicht

1. Das Sicherheitsdilemma von Wahlen
2. **IT-Sicherheit**
3. Die Werte der demokratischen Wahl
4. Wahlformen
5. Anforderungskatalog
6. GI-Wahlen 2004 und 2005

Sicherheit als Ausgleich von Interessenskollisionen

- Welche Teilnehmer?
- Welche Kommunikationsformen?
- Welche Interessen?
- Welche Interessenkonflikte?
- Wahlen fälschen, belauschen, verhindern?
- Wie ist das möglich?
- Wie kann das verhindert werden?

IT-Sicherheit (konstruktive Definition)

„Sicherheit“ ist die Eigenschaft eines Systems,
die dadurch gekennzeichnet ist,
daß die als bedeutsam angesehenen Bedrohungen,
die sich gegen die schützenswerten Güter richten,
durch besondere Maßnahmen so weit ausgeschlossen sind,
daß das verbleibende Risiko akzeptiert wird.

(REMO 1992)

Sicherheitsanalyse
z.B. BSI, CC

Die Werte und Bedrohungen von Wahlen

- Wahlen sind ein demokratisches Entscheidungsverfahren
- Freiheit und Mitbestimmung sind zentrale Werte
- In politischen Wahlen: Grundgesetz
- In nicht-politischen Wahlen: dieselben Grundsätze, aber mit jeweils abgeschwächten Sicherheitsbedürfnis
- Betrugsaufwand muss dem angestrebten Ergebnis entsprechen

Inhaltsübersicht

1. Das Sicherheitsdilemma von Wahlen
2. IT-Sicherheit
3. **Die Werte der demokratischen Wahl**
4. Wahlformen
5. Anforderungskatalog
6. GI-Wahlen 2004 und 2005

Es geht um mehr als Integrität und Anonymität

Vorbild Bundestagswahl (GG Art. 38):

- allgemein
- unmittelbar
- frei
- gleich
- geheim

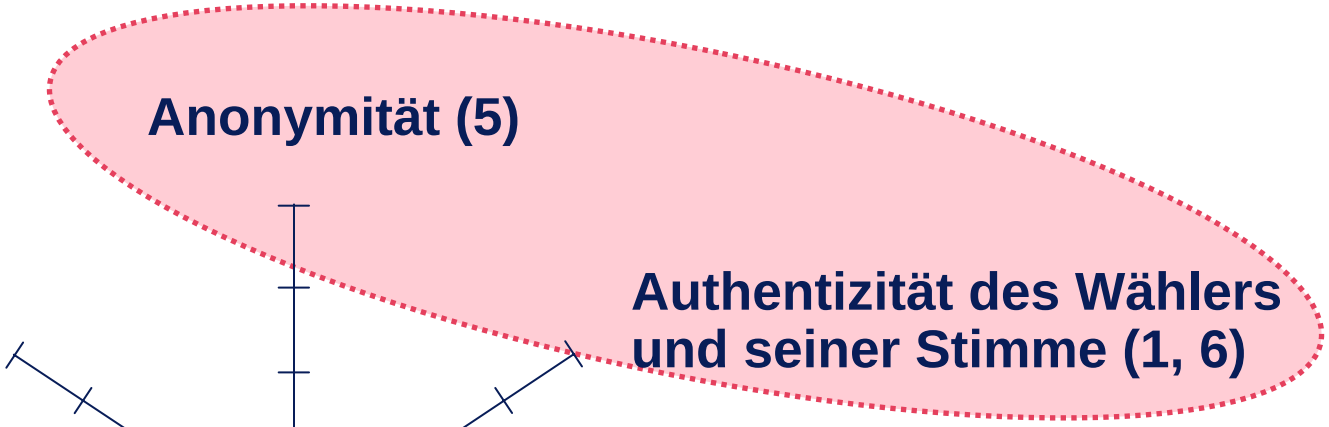
Gesetzliche Anforderungen ⇒ IT Sicherheit

allgemein	Zugang (1) Verfügbarkeit (2)	Ausschluss einzelner/Gruppen Sabotage/Ausfall
unmittelbar	(systembedingt, keine Mittler)	
frei	Kein gewaltsamer Einfluss (3)	Stimmenkauf/Erpressung
gleich	Funktionstreue des Systems (4)	Manipulation des Systems
geheim	Anonymität Vertraulichkeit (5) Nicht-Verknüpfbark.	Aufdecken des Wählerverhaltens

Gesetzliche Anforderungen ⇒ IT Sicherheit

allgemein	**Zugang (1)** **Verfügbarkeit (2)**	Ausschluss Sabotage/Ausfall
frei	**kein Einfluss (3)**	Stimmenkauf/Erpressung
gleich	**Funktionstreue des Systems (4)**	Manipulation d. Systems
geheim	**Anonymität** **Vertraulichkeit** **Nicht-Verknüpfb. (5)**	Aufdecken Wählerverhalten
(1)+(4)	**Fairness (6)**	Berechtigter ausgeschlossen Unberechtigter eingeschlossen Berechtigter mehr als 1x
Verant-wortung	**Nachvollziehbarkeit** **Kontrolle (7)**	Unstimmigkeiten nicht nachvollziehbar

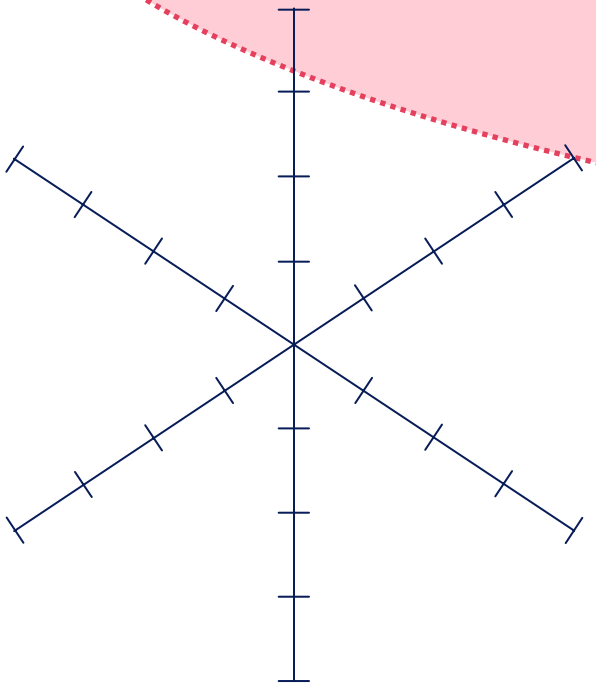
Das Wiener Anforderungs-Hexagramm



Anonymität (5)

Zugang, Verfügbarkeit (1,2)

Authentizität des Wählers und seiner Stimme (1, 6)



Nachvollziehbarkeit, Kontrolle (7)

Authentizität u. Funktions-treue des Systems (1, 4)

Freiheit / Nicht-Erpressbarkeit (3)

Based on: Posser, Kofler, Krimmer, Unger: Security Assets in E-Voting. In: Prosser, Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society. Workshop of the ESF TED Programme, 7-9 July 2004, Bregenz. Lecture Notes in Informatics, P-47, GI, Bonn 2004, 171-180, figs. 2 and 3.

Inhaltsübersicht

1. Das Sicherheitsdilemma von Wahlen
2. IT-Sicherheit
3. Die Werte der demokratischen Wahl
4. **Wahlformen**
5. Anforderungskatalog
6. GI-Wahlen 2004 und 2005

Wahlformen

	Präsenz	**Distanz**
Papier	Urne	Brief
Elektronik	Vernetzte Wahlgeräte im Wahllokal	Vernetzte Wahlgeräte im Kiosk *Home-PC/Internet*

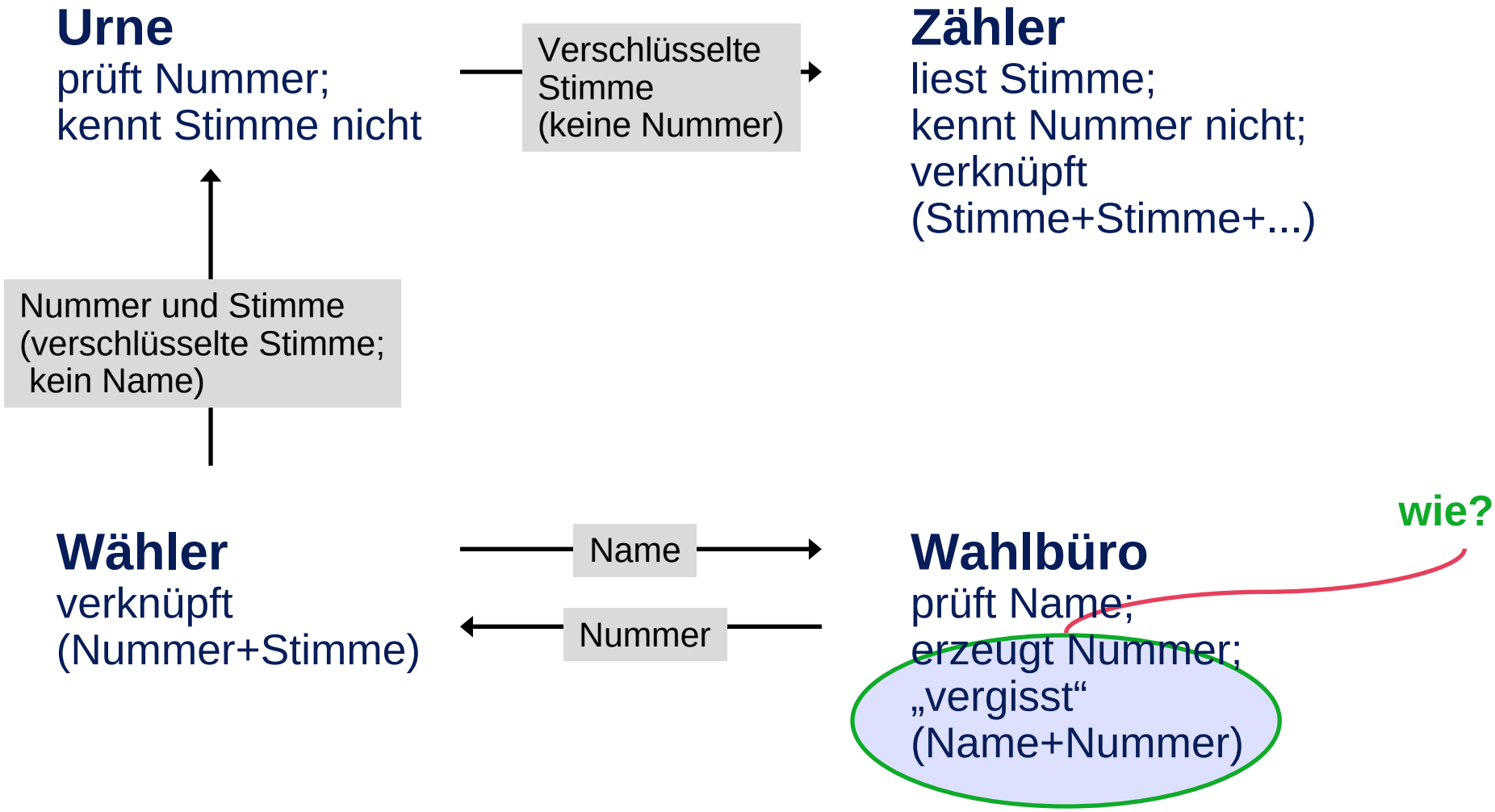
Nach Tab. 1 in Volkamer/Krimmer, Informatikspektrum April 2006

Internet-Wahlmodelle

- Pseudonymität und Aufgabenteilung
  - Aufgabenteilung Wahlbehörden und Urne
  - Trennung von Wähler-Id und Stimmen-Id
  - Wahlbehörde kennt Wähler-Id/Stimmen-Id und Urne Stimmen-Id/Stimme
- Blinde Signaturen
  - Wahlbehörde signiert blind eine Stimmen-Id oder eine Stimme
  - Perfekte Anonymität gegen über Wahlbehörde und Urne
- Verdeckte Auszählung
  - Runden von Stimmenabgabe und Stimmensammlung
  - Kryptographische Homomorphie
  - $\text{Encrypt}(T_1)*\text{Encrypt}(T_2)=\text{Encrypt}(T_1+T_2)$

Nach Volkamer/Krimmer, Informatikspektrum April 2006

z.B. Pseudonymität und Aufgabenteilung



Inhaltsübersicht

1. Das Sicherheitsdilemma von Wahlen
2. IT-Sicherheit
3. Die Werte der demokratischen Wahl
4. Wahlformen
5. **Anforderungskatalog**
6. GI-Wahlen 2004 und 2005

Anforderungskatalog

- Anforderungen an internetbasierte Vereinswahlen
- Entwickelt von GI-Expertenkreis für *GI-Wahlen*
- *Speziell* für Aufgabenteilung Register – Urne
- unter Verwendung von
  - PTB: Anforderungskatalog für Online-Wahlsysteme für nicht-parlamentarischen Wahlen
  - Council of Europe: Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting
  - IEEE P 1583TM, Draft 5.0: Standard for the Evaluation of Voting Equipment

Nach Informatikspektrum Oktober 2005

Anforderungskatalog

- Anforderungen an den Hersteller
  - Beschreibung, Analyse, Source-Code
- Anforderungen an die Wahlserver
  - Nachprüfbarkeit, 4-Augen-Prinzip, Aufgabenteilung

- Anforderungen an das Wahlsystem
  - Allgemeine Anforderungen
  - Bezug zu allgemeinen und gleichen Wahlen
    - Zugang, Fairness, Konsistenz
  - Bezug zu geheimen Wahlen
    - Anonymisierung, Pseudonymisierung, Nicht-Nachweisbarkeit
  - Ergonomie

Anforderungen an den Hersteller

- Systembeschreibung (Hard-/Software, Verfahren, Umgebungsbedingungen)
- Sicherheitsanalyse
- Source Code zur Prüfung
- Protokolle der Tests

- Bedienungsanleitungen – u.a. Schutz am Endgerät
- www.gi-ev.de/fileadmin/redaktion/Wahlen/handreichungen_gi_onlinewahlen2005.pdf

Anforderungen an die Wahlserver

- Sicheres Betriebssystem
- Vier-Augen-Prinzip und Aufgabenteilung bei allen Zugriffen
- Protokollierung aller Zugriffe

Anforderungen an das Wahlsystem

- Allgemeine Anforderungen
  - Korrekter Umgang mit Wahlunterbrechungen
  - Protokollierung des Wahlablaufs
  - Keine Funktion zur Zwischenergebnisberechnung
  - Abgleich Anzahl Wähler im WVZ und in der Urne

- Anforderungen bzgl. der gleichen u. allgemeinen Wahl
  - Ausschließen von Mehrfachstimmabgabe
  - Anzeige des integren und authentischen Stimmzettel
  - Konsistenzprüfung bei der Stimmenspeicherung
  - Korrekte Ergebnisberechung
  - Stimmen dürfen nicht unbemerkt gelöscht/verändert werden
  - Gleichheit bei der Stimmzetteldarstellung

Anforderungen an das Wahlsystem

- Anforderungen bzgl. der geheimen Wahl
  - Angemessenes Anonymisierungskonzept zur Wahrung des Wahlgeheimnisses
  - Anonymisierung zu allen Zeitpunkten gesichert: Abgabe, Transport, Speicherung, Auszählung
  - Keine Möglichkeit zum Nachweis über Wahlentscheidung

- Ergonomische und Bedienbarkeitsanforderungen
  - Verständlich und leicht handhabbar
  - Vorhandensein einer ausdrücklichen Bestätigungsfunktion

Verbleibende Probleme

- Auf praktikablem Sicherheitsniveau lösbar:
  - Anonymität, Integrität, Kontrolle, Korrektheit, Verfügbarkeit
- Verbleibende Probleme:
  - Transparenz und Vertrauen der Wähler
  - Präsentation an Nutzeroberflächen (z.B. Phishing, Farming)
  - Kollaboration bei 4-Augenprinzip und Aufgabenteilung
  - *Anhaltende* Unverknüpfbarkeit (trotz Internetspuren)
  - Kryptographische Algorithmen können gebrochen werden
- Erweiterungen:
  - Externe und interne Kontrollen
  - Zwischenergebnisse
  - Mehrfache Stimmabgabe

Common Criteria Protection Profile

- Sicherheitsanforderungen
  - zum Design eines Systems
  - zur Evaluierung eines Systems
  - zur Zertifizierung eines Systems
- Sicherheitsanforderungen
  - produktunabhängig
  - anwendungsunabhängig
  - Definition der Rahmenbedingungen und Voraussetzungen
  - Funktionale und organisatorische Mechanismen
  - Sicherheitsstufen
- Internationaler Standard
- Spezifikation eines CC PP für nicht-politische Online-Wahlen

Inhaltsübersicht

1. Das Sicherheitsdilemma von Wahlen
2. IT-Sicherheit
3. Die Werte der demokratischen Wahl
4. Wahlformen
5. Anforderungskatalog
6. **GI-Wahlen 2004 und 2005**

Historie der GI-Wahlen

- Dezember 2003: Erste elektronische Vereinswahlen der Initiative D 21
  - GI Geschäftsführung, Cornelia Winter: „Das können wir auch!“
  - GI-Gespräche mit D 21 und den dort beteiligten Partnern über ihre Erfahrungen
- Frühjahr 2004: Diskussion in Vorstand und Präsidium
  - Juni 2004: Positive Entscheidung.
- Anforderungen:
  - Einfache Handhabung
  - „So sicher wie Briefwahl“
  - Entscheidung für Micromata/Polyas mit User-Id und PIN
- Juli 2004: Einsetzen eines Expertenteams (Wahl- und Sicherheitsfachleute)
- Spätsommer 2004: Weiterentwicklung Software und Bedienbarkeit

Historie der GI-Wahlen

- September 2004: Präsidium beschließt Pilotversuch
- Oktober bis Dezember 2004: Präsidiumswahl reibungslos
- 2005: Entscheidung zur Fortsetzung Präsidiums- und Vorstandswahlen 2005
- Fortsetzung des Expertenteams 2005
- Oktober bis Dezember 2005: Präsidiums- und Vorstandswahl reibungslos

Wer hat was gemacht?

- Initiierung durch Geschäftsstelle (C. Winter)
- Vorstand und Präsidium lassen sich überzeugen
- Expertenteam für Wahlen und Sicherheit (Brunnstein, Grimm, Pfitzmann, Richter)
- Codereview durch GI-Mitglieder
- Juristische Begleitung durch Rechtsanwältin Kiani (Wahlleitung)
- Zusammenarbeit mit Partner Micromata (win-win)
- organisatorische Begleitung Mas (Vizepräsident) und Winter (Geschäftsstelle)
- Testwahl in mehreren Iterationen (GI-Mitglieder)
- Wahlbeobachtung am Wahlserver

Was hat es gebracht? (C. Winter)

- Verdoppelung der Wahlbeteiligung
- Erstellung und Veröffentlichung eines ersten Anforderungskatalogs für elektronische Wahlen (Vorbildcharakter)
- großes Interesse seitens einiger Ministerien und anderer Vereine/Verbände
- GI hat sich als Vorreiterin positioniert und Mut bewiesen
- Sachverstand unserer Fachleute hat Verfahren vertrauenswürdig gemacht
- Wiederbelebung der Diskussion auf der Basis einer realen Erfahrung und eines realen Systems
- Vorbereitung des „Wahlalltags“ in den Fachbereichen und Fachgruppen der GI

Ergebnisse GI Onlinewahlen 2004 und 2005

- ca. 20.000 Wahlberechtigte
- Briefwahlen vor 2004
  - 10-15%
- GI Präsidium Okt-Dez 2004
  - 4.845 Stimmen
  - 24%
- GI Vorstand und Präsidium Okt-Dez 2004
  - 4.030 Stimmen
  - 20%

Was bleibt zu tun?

- Weiterentwicklung des Systems
  - Verbesserung von Recovery
  - Einfachere Entdeckung und Behebung von Inkonsistenzen
  - Vereinfachung der Verteilung von Zugangsberechtigungen
  - Resistenz gegen DDoS-Attacks
  - Resistenz gegen SW-Fehler und Traps
- CC Protection Profile
- Zertifizierung mehrerer Systeme
- Integration in andere Kommunikationsformen (E-Mail, E-Conferencing, CSCW)
- Lernen aus den E-Vote-Sicherheitslösungen für andere Kommunkationsformen
- Einführung in den Alltag der Universitäten, Gremien, Administrationen, … politische Wahlen

Vielen Dank und…

- Empfehlung zur weiteren Literatur

- PTB: Anforderungskatalog für Online-Wahlsysteme für nicht-parlamentarischen Wahlen. April 2004. http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf
- Council of Europe: Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Sep 2004.
- IEEE P 1583TM, Draft 5.0: Standard for the Evaluation of Voting Equipment. 2005. http://grouper.ieee.org/groups/scc38/index.htm

- Winter: GI Anforderungskatalog, Informatikspektrum, Oktober 2005.
- Volkamer/Krimmer: Die Online-Wahl auf dem Weg zum Durchbruch. Informatikspektrum April 2006.
- Grimm/Krimmer/Meißner/Reinhard/Volkamer/Weinand: Security Requirements for Non-political Electronic Voting. *Submitted to* Electronic Voting in Europe – Technology, Law, Politics and Society. Workshop of the ESF TED Programme, July 2006, Bregenz.