Science meets Politics

E-Voting in der Schweiz

Wie weiter?

17. März 2011

Prof. Eric Dubuis / Prof. Rolf Haenni

Research Institute for Security in the Information Society
Berner Fachhochschule, Technik und Informatik, Biel

Wer / wo / warum / wie?

- Wer sind wir?
- Wo stehen wir heute?
  - in der Schweiz
  - im Ausland
  - in der Forschung
- Warum braucht es Verifizierbarkeit?
- Wie weiter?

Wer sind wir?

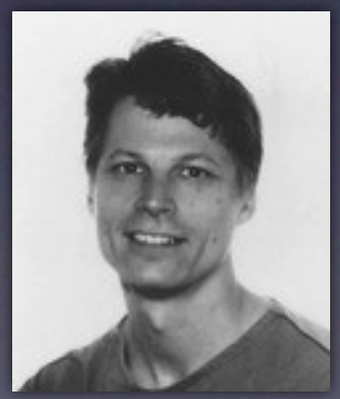
Wer sind wir?

- Forschungsgruppe seit 2008
  - elektronische Wahlen und Abstimmungen
  - Kryptographie
  - IT-Sicherheit
- 3 Professoren, 2 Doktoranden, 1 Assistent

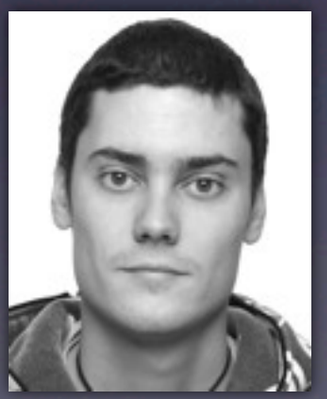

Eric Dubuis


Rolf Haenni


Stephan Fischli


Reto Koenig


Oliver Spycher


José Beuchat

Wer sind wir?

- Projekte
  - FIDIS (EU FP6, 2004-2009)
  - TrustVote (BFH, 2008-2009)
  - SwissVote (Hasler-Stiftung, 2009-2012)
- Publikationen (seit 2007)
  - 7 internationale Konferenzen
  - 2 Fachartikel
  - 2 technische Berichte
  - weitere Publikationen in der Pipeline

Wer sind wir?

- Swiss E-Voting Workshop (mit BK, Uni FR)
  - 2009: ca. 60 Teilnehmer, mehrheitlich CH
  - 2010: ca. 65 Teilnehmer, ca. 30% Ausland
- Baloti.ch (mit ZD Aarau)
  - Abstimmungsplatform für Immigranten in der CH
  - 3 Abstimmungen seit 2010
  - eventuell Wahlen 2011
- E-Voting Competence Center
  - Gründung Fachverein 2011

Wo stehen wir heute?

in der Schweiz

Wo stehen wir heute?

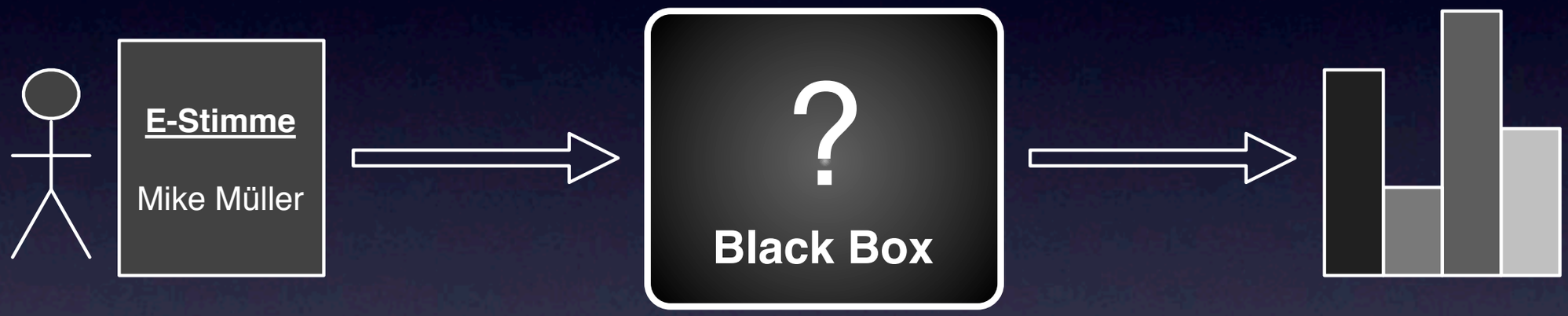
- Pionierrolle CH
- 3 Systeme im Einsatz (seit 2003)
  - Genf (Eigenentwicklung)
  - Zürich (Unisys)
  - Neuenburg (Scytl)
- “Beherbergung” anderer Kantone
  - Genf: BS, LU, (BE)
  - Zürich (Unisys): FR, SO, SH, SG, GR, AG, TG
- Max. 10% E-Stimmen auf Bundesebene

Wo stehen wir heute?

- Die CH-Systeme sind “Black Box”-Systeme

Wo stehen wir heute?

- Die CH-Systeme sind “Black Box”-Systeme



- Fragen
  - Wurde meine Stimme gezählt?
  - Wurde richtig zusammengezählt?
  - Wurden nur gültige Stimmen gezählt?

Wo stehen wir heute?

- GE: E-Voting von Bevölkerung gutgeheissen (2009)
- BL: Motion "Mohn" (2010)
  - "*Die Pilotprojekte [...] haben gezeigt, dass E-Voting nicht nur machbar, sondern auch sicher ist. So stellen die Sicherheitsrisiken heute keine unüberwindbaren Schranken mehr dar.*"
- VD: Motion "Schwaab" (2010)
  - "*Ainsi, le vote électronique entraîne un risque de fraude important. [...] Un seul pirate informatique [...] peut modifier le résultat d'un scrutin sans que cela ne laisse de trace [...].*"

Wo stehen wir heute?

im Ausland

Wo stehen wir heute?

HOLLAND

- Einsatz von Wahl-Computern (seit 1965!)
- Verletzlichkeit des Systems öffentlich vorgeführt (2006)
- Innenministerium enzieht Zulassung (2007)
- Ministerrat beschliesst, künftig nur noch Papier-Wahlen zu erlauben (2008)

Wo stehen wir heute?

DEUTSCHLAND

- Einsatz von Wahl-Computern für Bundestagswahl (2005)
- Entscheid Bundesverfassungsgericht (2009)
  - > "*Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig [...] überprüft werden können.*"
- Umfassendes Verbot elektronischer Wahlgeräte

Wo stehen wir heute?

NORWEGEN

- Entwicklung in Auftrag gegeben (Scytl)
- Ziele
  - Erfüllen der "*Guidelines on transparency of e-enabled elections*" (Europarat, 2010)
  - Fehler anderer Länder vermeiden
- 6 Probeläufe durchgeführt
- Kommunal- und Bezirkswahlen im Herbst 2011

Wo stehen wir heute?
in der Forschung

Wo stehen wir heute?

- Ca. 150 technische Fachartikel (seit 1988)
- Viele nicht-technische Fachartikel
- 6 spezialisierte internationale Konferenzen
  - VoteID
  - EVT/WOTE
  - EVOTE
  - REVOTE
  - SecVote
  - Swiss E-Voting Workshop

Wo stehen wir heute?

- Existierende Systeme
  - Helios (USA, Belgien)
  - Civitas (USA)
  - Scantegrity (USA)
  - Prêt-à-Voter (Luxemburg, UK)
  - Selectio Helvetica (CH, in Entwicklung)
- Die Korrektheit der Ergebnisse ist öffentlich *verifizierbar*

Wo stehen wir heute?

- Das “perfekte” System existiert (noch) nicht
- Offene Probleme
  - sichere Plattform (siehe ETHZ-Studie)
  - Stimmenkauf und Erpressung (Ansätze existieren, aber ineffizient)
  - Langzeit-Sicherheit
  - Usability komplexer Kryptographie
- Viele Kryptographen raten davon ab, E-Voting heute schon in der Praxis einzusetzen

Warum braucht es Verifizierbarkeit?

Warum Verifizierbarkeit?

Das “perfekte” E-Voting System garantiert ...

- Geheimnis der Wahl
  - keine Verknüpfung zw. Stimmen und Stimmenden
- Freiheit der Wahl
  - kein Stimmenkauf
  - keine Erpressung oder Nötigung
  - kein “Family-Voting”

Warum Verifizierbarkeit?

Das “perfekte” E-Voting System garantiert ...

- Korrektkeit der Wahl
  - nur Berechtigte können stimmen
  - niemand kann mehr als einmal stimmen
  - abgegebene Stimmen sind nicht veränderbar
  - alle abgegebenen Stimmen werden gezählt

Warum Verifizierbarkeit?

Das “perfekte” E-Voting System garantiert ...

- Korrektkeit der Wahl
  - nur Berechtigte können stimmen
  - niemand kann mehr als einmal stimmen
  - abgegebene Stimmen sind nicht veränderbar
  - alle abgegebenen Stimmen werden gezählt
- Verifizierbarkeit der Wahl
  - Korrektheit kann öffentlich überprüft werden

Warum Verifizierbarkeit?

- Verifizierbarkeit durch “transparente Urne”
  - Stimmen erscheinen auf einem “elektronischen Anschlagbrett”
  - sämtliche Schritte der Wahladministration werden offengelegt
  - ... und können nachgerechnet werden

Warum Verifizierbarkeit?

- Verifizierbarkeit ...
  - impliziert die Korrektheit des Resultats
  - minimiert das nötige Vertrauen in die Betreiber
  - erhöht das Vertrauen der Wählerschaft ins System
  - vereinfacht das Behandeln von Beschwerden
  - wird von der Wissenschaft gefordert

Wie weiter?

Wie weiter?

1. Mit bestehenden Systemen

- Vorteile
  - minimale Kosten
  - Infrastruktur existiert
- Nachteile
  - Sicherheitsbedenken bleiben bestehen
  - Kritik internationaler Experten möglich
  - Verlust Pionierrolle

Wie weiter?

II. Bestehende Systeme verbessern

- Vorteile
  - > geringe Kosten
  - > Infrastruktur existiert
- Nachteile
  - > Verbesserungen nur punktuell möglich
  - > nicht alle Eigenschaften realisierbar

Wie weiter?

III. Verifizierbares System entwickeln

- Vorteile
  - garantiert korrekte Resultate
  - Stand der Forschung
  - Pionierrolle fortführen
- Nachteile
  - unbekannte Kosten
  - unbekannte Entwicklungszeit

Wie weiter?

IV. Übungsabbruch

- Vorteile
  - keine Kosten
  - kein Risiko
- Nachteile
  - technologischer Rückschritt
  - verlorene Investitionen
  - Verlust Pionierrolle

Fragen und Diskussion

(mehr Informationen auf http://e-voting.bfh.ch)