DACHS-Symposium 2012, Biel, Schweiz

Elektronische Wahlsysteme: Chance oder Risiko?

25. September 2012

Rolf Haenni

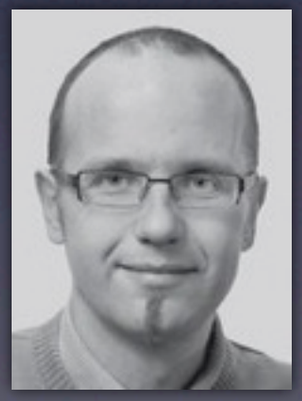
Berner Fachhochschule – Research Institute for Security in the Information Society

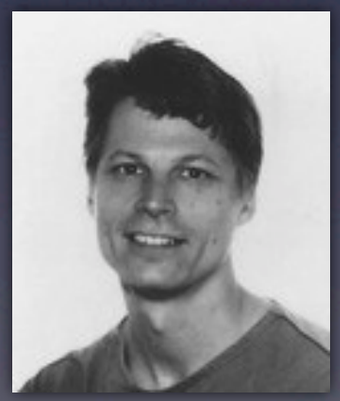
Wer sind wir?

- Forschungsgruppe an der BFH seit 2008
- Thema: Sichere Internetwahlen
- 4 Professoren, 2 Doktoranden, 2 Assistenten

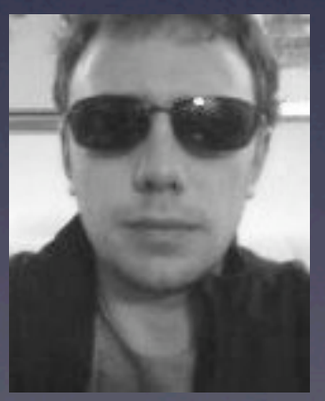

Eric Dubuis


Stephan Fischli


Rolf Haenni


Reto Koenig


Oliver Spycher


Severin Hauser

Aktivitäten

- Swiss E-Voting Workshop (2009, 2010, 2012)
- E-Voting Competence Center (2011)
- E-Voting Projekte
  - FIDIS (EU-FP6), 2004-2009
  - TrustVote (BFH), 2008-2009
  - SwissVote (Hasler Stiftung), 2009-2012
  - Baloti.ch (ZDA), 2010-2012
  - UniVote (SUB/BFH), 2012-2013
  - VIVO (SNF/FNR), 2012-2014
- Zahlreiche wissenschaftliche Publikationen

Inhaltsverzeichnis

Gefahren bei Internetwahlen

Le Matin

Un citoyen a pu voter deux fois

INTERNET — Le système de vote électronique a permis à un électeur de voter à double ce week-end. La Chancellerie fédérale se veut rassurante, mais pour le Parti pirate, ce couac décrédibilise l'e-voting.

Par Simon Koch. Mis à jour le 12.03.2012

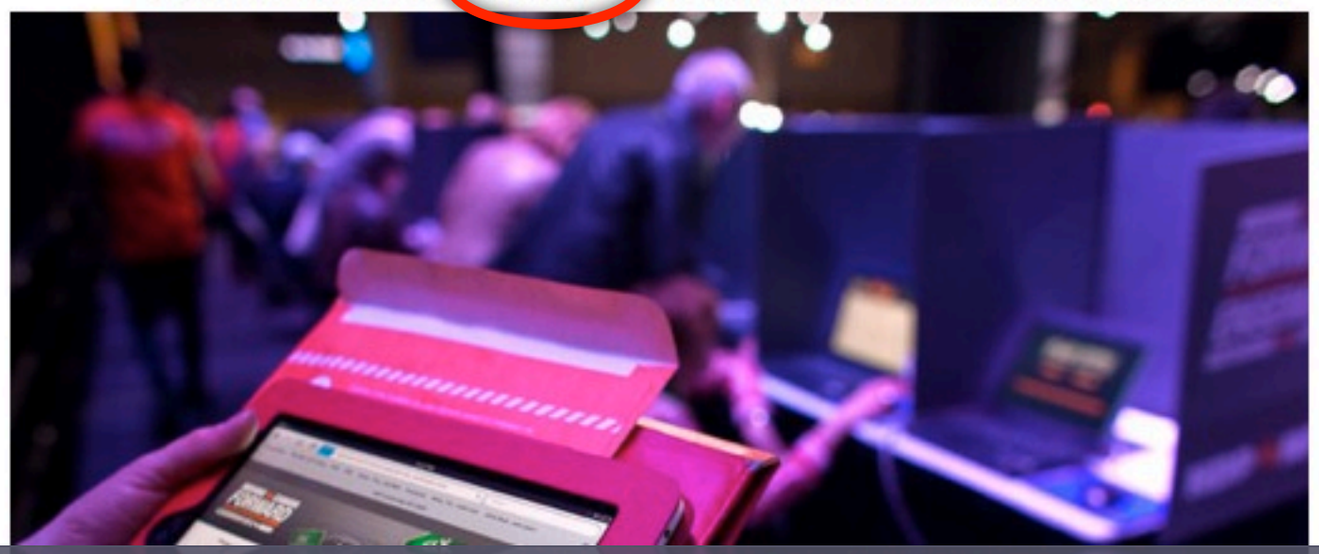
33 Commentaires

NATIONAL POST

NEWS

Cyber attack on NDP leadership vote involved more than 10,000 computers

National Post Staff | Mar 27, 2012 2:07 PM ET | Last Updated: Mar 27, 2012 1:44 PM ET



L'INFORMATICIEN

Législatives : 130 000 Français ont voté dangereusement par Internet

par Emilien Ercolani, le 30 mai 2012 11:57

Les Français de l'étranger, qui peuvent voter par Internet depuis le 23 mai, ont été potentiellement la cible de détournements de leurs votes. Malgré la dénonciation d'une possible faille lors du vote, rien ne semble avoir bougé.

Décidément, le vote autre que sur un morceau de papier a du mal à rassurer, et encore… Déjà en 2007, nous relayions dans un papier **les alertes des informaticiens** concernant le vote électronique (des machines dans les urnes). Aujourd'hui, c'est le vote par Internet qui est la cible de menaces. Et pour la première année, les Français de l'étranger avaient la possibilité d'utiliser ce moyen.

Sur le papier, la démarche est excellente, puisqu'elle évite de se déplacer dans des bureaux de vote. En revanche, la presse fait état de gros problèmes de sécurité qui d'une part n'ont pas été réglés, d'autre part ont été presque ignorés. Pourtant, dans un **document d'une vingtaine de pages** (ci-dessous) assorti d'une vidéo en situation réelle, le développeur Laurent Grégoire démontre par A + B comment il est possible de détourner un vote : vous votez pour monsieur X, et c'est finalement madame Y qui reçoit votre vote.

Une attaque relativement simple

Le document, intitulé « Comment mon ordinateur a voté à ma place (et à mon insu) », est très

Potentielle Gefahren

- Fehlerhaftes System oder Bedienung
- Angriff auf das zentrale System
  - Denial-of-Service
  - Eindringen in Server oder DB
  - Code-Injection
- Angriff auf die Computer der WählerInnen
  - Spyware, Keylogger, etc.
  - Man-in-the-Browser
- Angriff auf beteiligte Personen (Bestechung, etc.)

Profil eines Angreifers

- Voraussetzung 1: Motivation
  - Beinflussung des Resultats
  - Behindern einer Wahl
  - Diskreditierung des Systems oder der Betreiber
  - Verhindern von E-Voting
  - Persönliche Herausforderung, Profilierung oder Bereicherung
- Voraussetzung 2: Fachwissen
  - Hacker-Szene, Chaos Computer Club, etc.
  - Umfeld Forschung & Wissenschaft
  - Insider: aktuelle & ehemalige Mitarbeiter

Ist E-Voting vertrauenswürdig?

- Können die verschiedenen Angriffs-Szenarien verhindert werden?
- Können erfolgreiche Angriffe entdeckt werden?
- Kann die Wählerschaft überzeugt werden, dass kein Angriff stattgefunden hat?
  - Berücksichtigung der eigenen Stimme
  - Korrektheit des Resultats
  - Gewährung des Stimmgeheimnisses

Einsatz elektronischer Wahl-Systeme

in der Schweiz

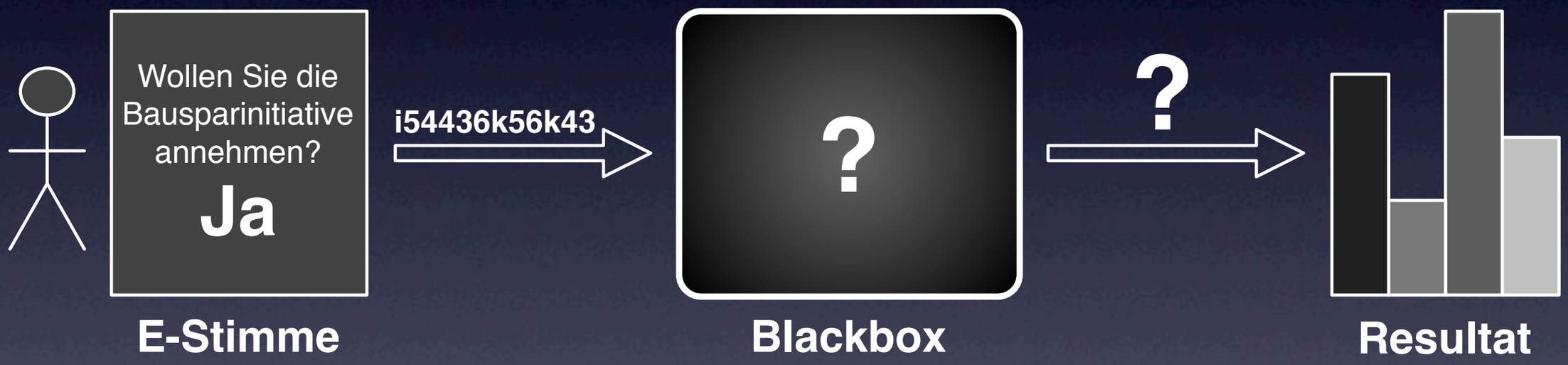
Aktuelle Systeme

- Seit 2003 sind 3 Systeme im Einsatz
  - Genf
  - Zürich (Unisys)
  - Neuchâtel (Scytl)
- “Beherbergung” von anderen Kantonen
  - Genf beherbergt 3 Kantone
  - Zürich beherbergt 5 Kantone
- Beschränkung des Elektorats auf 10%

Klassischer Ansatz

- Persönliche Zugangsdaten per Post
- Stimmabgabe mittels Web-Applikation
  - > Stimme wird erfasst und verschlüsselt (Javascript)
  - > Wahlberechtigung mittels Zugangsdaten
  - > Verschlüsselte Stimme wird an Server geschickt
  - > "*Ihre Stimme wurde erfolgreich empfangen*"
- Veröffentlichung des Resultats

“Blackbox”-Wahlsystem



Nachteile

- Postkanal erforderlich
- Abstimmungsdaten müssen geschützt werden
- Server-Infrastruktur muss geschützt werden
- Client-Computer müssen geschützt werden
- Keine Nachvollziehbarkeit & Transparenz
- Hohes Mass an Vertrauen erforderlich

Einsatz elektronischer Wahl-Systeme

in Europa

Holland

- seit 1965 : Einsatz von Wahlcomputern
- 2006 : Erfolgreicher Angriff öffentlich vorgeführt
- 2007 : Innenministerium enzieht Genehmigung
- 2008 : Ministerrat beschliesst, zu Papierwahlen zurückzukehren

Deutschland

- 2005 : Bundestags-Wahl mit Wahlcomputern
- 2009 : Deutsches Verfassungsgericht:

  "*Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig [...] überprüft werden können.*"
- Umfassendes Verbot von elektronischen Wahlen

Norwegen

- 2009 : Entwicklung eines Internet-Wahlsystems
- Ziele
  - Erfüllen der “Guidelines on Transparency of E-Enabled Elections” (Europarat, 2010)
  - Zusammenarbeit mit der Wissenschaft
  - Aus Fehlern lernen
- 2011: Kommunale und regionale Wahlen

Internet-Wahlen in der Forschung

E-Voting Forschung

- >200 technische Publikationen (seit 1988)
- Viele nicht-technische Publikationen
- >6 spezialisierte interntionale Konferzen
  - VoteID
  - EVT/WOTE
  - EVOTE
  - REVOTE
  - SecVote
  - Swiss E-Voting Workshop

Existierende Systeme

- Existierende Implementierungen
  - Helios (USA, Belgien)
  - Civitas (USA)
  - Scantegrity II (USA)
  - Prêt-à-Voter (Luxembourg, UK)
  - Baloti.ch (Scheiz)
  - UniVote (Schweiz, ab 2013)
- Wenig Erfahrung mit echten Wahlen

Technlogien

- Standard Kryptografie
  - Verschlüsselung
  - Digitale Unterschriften
- “Advanced”-Kryptografie
  - Homomorphes Zählen
  - Blinde Signaturen
  - Secret Sharing
  - Schwellwert-Kryptosysteme
  - Verifizierbare Mix-Netzwerke
  - Zero-Knowledge Beweise

Aktueller Stand

- Es gibt kein “perfektes” System
- Offene Probleme
  - Sicherheit beim Client-Computer
  - Stimmenkauf und Erpressung
  - Langzeit-Sicherheit
  - Benutzbarkeit komplexer Kryptografie
- Viele namhafte Kryptografen lehnen Internet-Wahlen ab

Verifizierbarkeit

Verifizierbarkeit

- Sämtliche Abstimmungsdaten sind öffentlich
  - Verschlüsselte Stimmen
  - Digitale Signaturen
  - Kryptografische Beweise für korrektes Mischen und Entschlüsseln
- Das Resultat ergibt sich aus kryptografischen Berechnungen auf den Abstimmungsdaten

“Glass Box”-Wahlsystem

Vorteile

- Berücksichtigung der eigenen Stimme überprüfbar
- Ermittlung des Resultats nachvollziehbar und nachprüfbar
- Erleichterter Schutz der Abstimmungsdaten
- Erleichtertes Erkennen von Fehlern oder Manipulationen

Fazit und Ausblick

Fazit

- Sichere Internetwahlen sind hochkomplex
- Grosse Fortschritte in der Forschung
- Praxis hinkt Forschung hinterher
- Forderungen der Forschung:
  - Verifizierbarkeit (individuell & universell)
  - Transparenz (Dokumentation, Code, etc.)
  - Verteilung von “Macht” auf verschiedene Personen
- Es gibt kein “perfektes” System

Ausblick

- Offene Probleme
  - Stimmenkauf und Erpressung
  - Langzeit-Sicherheit
  - Unsichere Client-Computer
  - Benutzbarkeit komplexer Kryptografie
- Chance oder Risiko?

Fragen?

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