Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

# Der Client als Achilles-ferse beim Remote Internet Voting

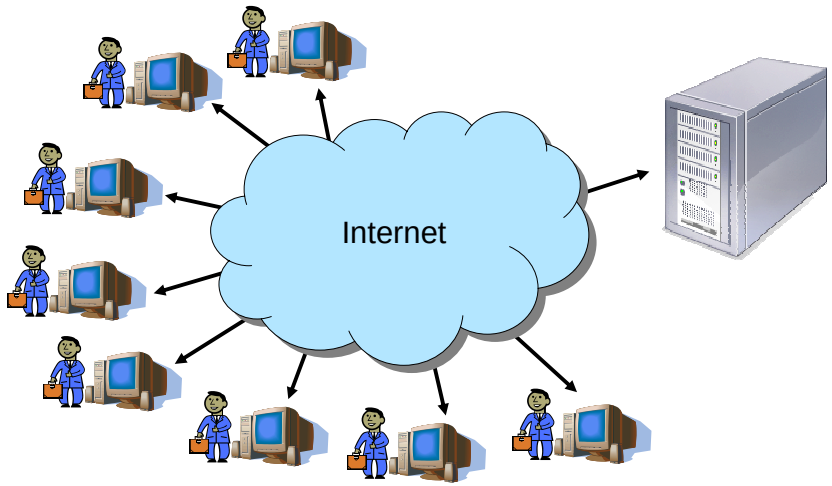
Rolf Oppliger
Informatikstrategieorgan Bund ISB
Swiss E-Voting Workshop, 5. Juni 2009

## Ausgangslage

- Beim **vote éléctronique** geht es unter anderem um die Teilnahme von stimmberechtigten Personen an Abstimmungen und/oder Wahlen mit Hilfe von informations- und kommunikationstechnischen Mitteln
- Formen des **Internet-basierten vote éléctronique**
  - Poll-site Internet Voting
  - Kiosk Voting
  - ➢ Remote Internet Voting
- Entsprechende **Pilotversuche** werden in den Kantonen Genf, Zürich und Neuenburg durchgeführt



## Remote Internet Voting






## Sicherheitsfragen im Zusammenhang mit dem Remote Internet Voting

- Gegenseitige Authentifikation (bzw. Autorisation) von stimmberechtiger Person und Abstimmungsserver
- Gesicherte Kommunikation durch das Internet
- ➢ Gesicherte Stimmabgabe auf dem Client

- Demokratische Kontrolle des Auszählprozesses (verteiltes Vertrauen)
- Nachvollziehbar- und Beweisbarkeit (idealerweise End-zu-End)

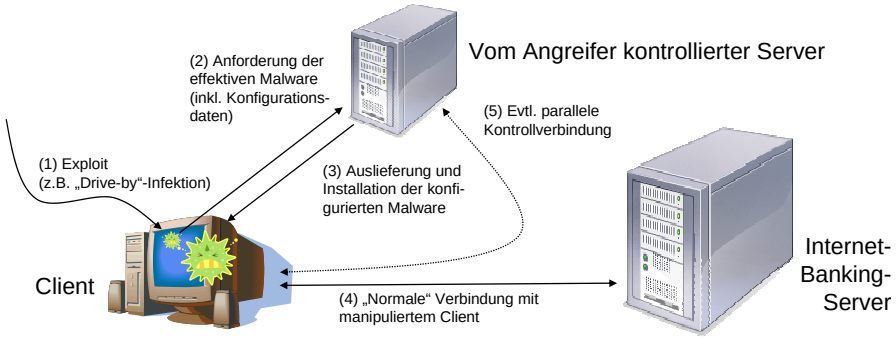
# Client-seitige Sicherheit 1/4

**Feststellung 1:** Wer die Benutzerschnittstelle kontrolliert, kontrolliert auch die Stimmabgabe




# Client-seitige Sicherheit 2/4

**Feststellung 2:** In vielen Web-basierten Anwendungen ist die Benutzerschnittstelle bereits unter Beschuss bzw. Kontrolle der Angreifer (z.B. Internet-Banking)






# Client-seitige Sicherheit 3/4

- Client-seitige Angriffe sind technisch möglich und finden statt (im Rahmen von Malware-, „Browser Poisoning"- bzw. „Man-in-the-Browser"-Angriffen)
- Ob eine Internet-Banking-Transaktion oder eine im Rahmen von Remote Internet Voting abgegebene Stimme manipuliert wird ist irrelevant
- Das Manipulieren einer Stimme ist eher einfacher, weil keine parallele Kontrollverbindung erforderlich ist
- Im Fall von Remote Internet Voting erschweren oder verunmöglichen Anonymitätsanforderungen (Stimmgeheimnis) die Nachvollziehbar- und Beweisbarkeit



# Client-seitige Sicherheit 4/4

- Die Bedrohungslage ist erheblich
- Grossflächige Angriffe sind technisch möglich (z.B. im Rahmen von Botnets)
- Die Risiken hängen von der Bedeutung und Tragweite der angegriffenen Abstimmung oder Wahl ab (Analogie: Geldtransport)
- Auf der einen Seite bietet das politische System der Schweiz (direkte Demokratie) zwar nur schwache Anreize für potentielle Angreifer …
- … auf der anderen Seite können Angriffe aber auch nicht wirksam verhindert werden

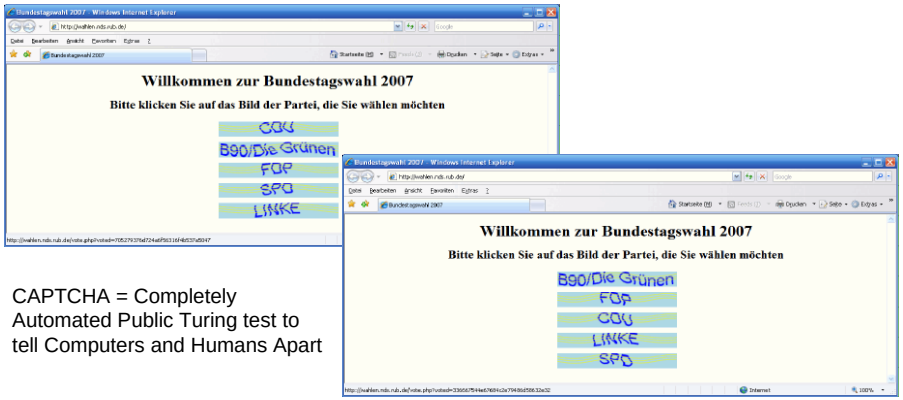
# Lösungsansätze 1/3

- Im Internet-Banking werden vermehrt Transaktionsauthentifikations- und -überwachungsverfahren (Monitoring) eingesetzt
- Solche Verfahren können im Remote Internet Voting nicht direkt eingesetzt werden (aufgrund von Anonymitätsanforderungen)
- Code Voting stellt einen alternativen Lösungsansatz dar
- Beim Code Voting erfolgt die Stimmabgabe über Benutzer-spezifische Pseudozufallscodes (z.B. 8212 für JA und 2123 für NEIN)



# Lösungsansätze 2/3

- Mit Hilfe von CAPTCHAs kann die Benutzerfreundlichkeit von Code Voting verbessert werden




CAPTCHA = Completely Automated Public Turing test to tell Computers and Humans Apart



# Lösungsansätze 3/3

- Auch im Zusammenhang mit (CAPTCHA-basiertem) Code Voting sind noch viele Fragen unbeantwortet
  - Juristische Akzeptanz
  - Benutzbarkeit bzw. Benutzerfreundlichkeit (insbesondere bei Wahlen)
  - Sicherheit von CAPTCHAs
  - …
- Möglicherweise bieten die auf internationaler Ebene diskutierten End-zu-End (E2E) verifizierbaren Abstimmungs- und Wahlverfahren alternative oder komplementäre Lösungsansätze an



# Schlussfolgerungen und Ausblick

- Insbesondere auf der Client-Seite gibt es im Remote Internet Voting noch viele Sicherheitsprobleme
- Die Lösung dieser Probleme erfordert zum Teil auch neue Lösungsansätze
- Solche Lösungsansätze werden im Rahmen einer Forschungszusammenarbeit zwischen BK, ETHZ und ISB untersucht
- In der Zwischenzeit ist eine defensive Haltung angebracht und eine Beschränkung des Elektorats sinnvoll
- Zunehmend viele Staaten wenden sich sogar vom Einsatz von Wahlcomputern ab