The European eID Interoperability Concepts and Compliance Conference

Privacy and Integrity in Internet Voting

Problems & Solutions

March 27th, 2012

Prof. Rolf Haenni

Research Institute for Security in the Information Society
Bern University of Applied Sciences

Content

- Introduction
- Internet Voting Today
  - in Switzerland
  - in other countries
  - in research
- Verifiability
- Conclusion

Who are we?

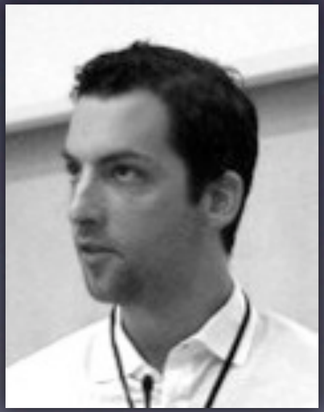
- Research group since 2008
  - Secure Internet voting
  - Cryptographic protocols
  - Privacy enhancing technologies
- 4 professors, 2 PhD students, 2 assistants

Eric Dubuis

Rolf Haenni

Stephan Fischli

Reto Koenig



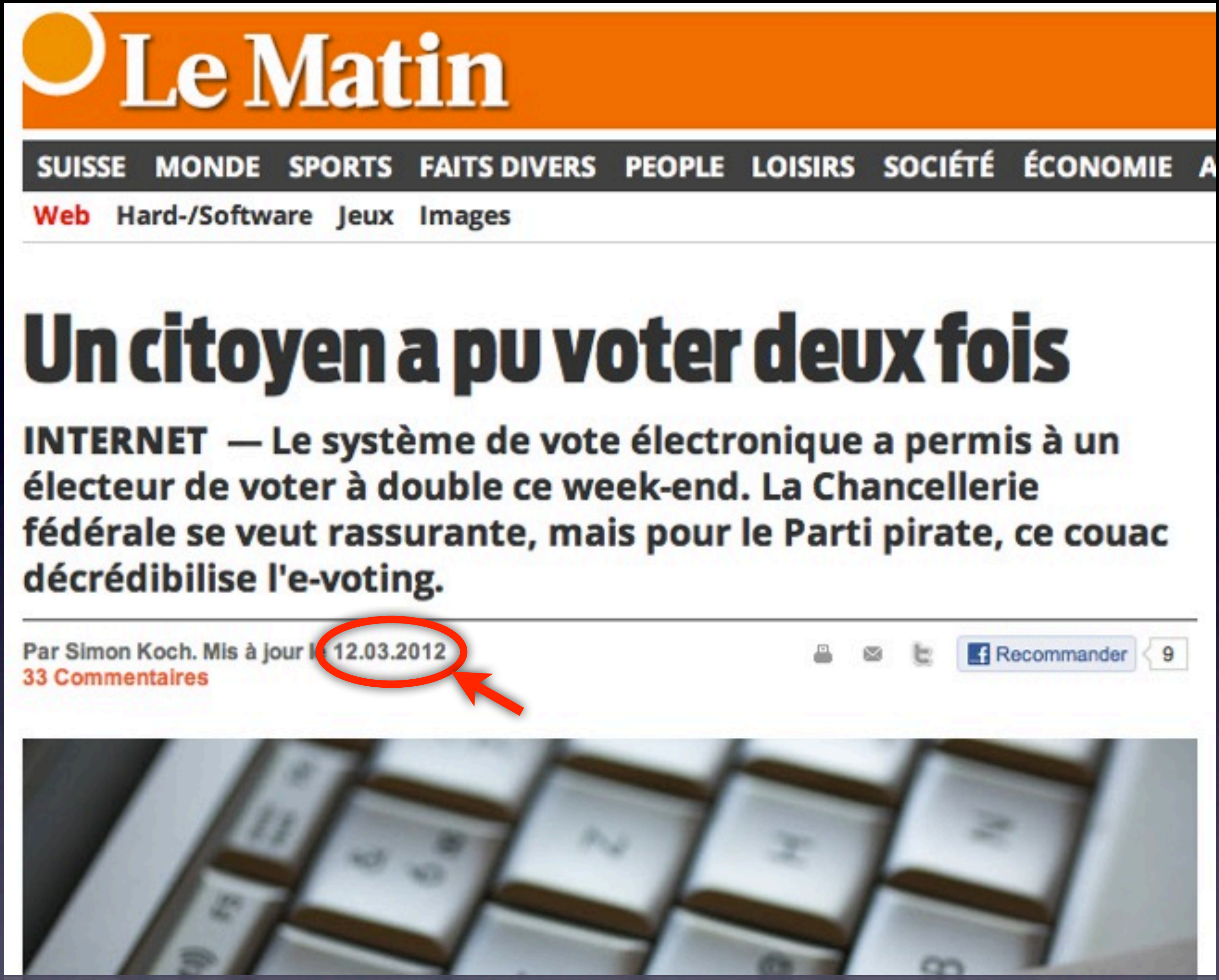
Oliver Spycher

Severin Hauser

Who are we?

- Projects
  - FIDIS (EU-FP6, 2004 - 2009)
  - TrustVote (BFH, 2008 - 2009)
  - SwissVote (Hasler Foundation, 2009 - 2012)
  - Baloti.ch (2010 - 2012)
  - UniVote (2012 - ?)
- Numerous scientific publications
- Swiss E-Voting Workshop (2009 / 2010 / 2012)
- E-Voting Competence Center (founded in 2011)

Introduction


Le Matin
SUISSE MONDE SPORTS FAITS DIVERS PEOPLE LOISIRS SOCIÉTÉ ÉCONOMIE A
Web Hard-/Software Jeux Images
Recommander 9

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

“A citizen was able to vote twice”

Questions

- Which of the two votes was counted?
- How does the “monitoring system” work?
  - Does it detect all possible irregularities?
  - Does it guarantee the secrecy of the vote?
  - Who monitors the monitoring system?
- How trustworthy is an erroneous system?
  - Is the detection of errors a good or a bad sign?
  - How many (other) bugs does it have?
  - Is open-source software more trustworthy?

General Requirements

A “perfect” Internet voting system guarantees ...

- Privacy
  - votes can not be linked to voters
  - voters can vote anonymously
- Coercion-Resistance
  - no vote buying
  - no coercion of voters (e.g. “family-voting”)
- Fairness
  - no partial results are revealed

General Requirements

A “perfect” Internet voting system guarantees ...

- Correctness
  - only eligible voters can vote
  - nobody can vote more than once
  - submitted votes can not be altered
  - all valid votes are counted
- Verifiability
  - correctness can be publicly verified (by anyone)

General Requirements

A “perfect” Internet voting system guarantees ...

- Correctness
  - only eligible voters can vote
  - nobody can vote more than once
  - submitted votes can not be altered
  - all valid votes are counted
- Verifiability
  - correctness can be publicly verified (by anyone)

Internet Voting Today

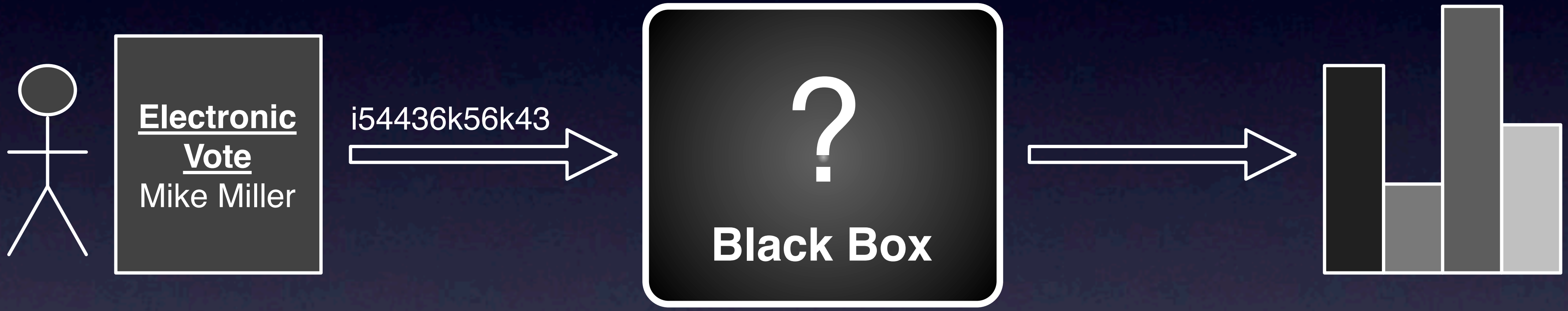
in Switzerland

Internet Voting Today

- Three different systems since 2003
  - Geneva
  - Zürich (Unisys)
  - Neuchâtel (Scytl)
- Service for other cantons
  - Geneva hosts 3 cantons
  - Zürich (Unisys) host 5 cantons
- Max. 10% electronic votes on federal level

Internet Voting Today

- All Swiss systems are “black boxes”



- Questions
  - Has my vote been counted correctly?
  - Have only valid votes been counted?
  - Have all valid votes been counted?

Internet Voting Today

in other countries

(Internet) Voting Today

THE NETHERLANDS

- Election computers widely used (since 1965)
- Vulnerability of system exposed in public (2006)
- Ministry of the interior removed permission (2007)
- Council of ministers decided to fully return to paper-based elections (2008)

(Internet) Voting Today

GERMANY

- Computers used for Bundestag election (2005)
- Federal Constitutional Court (2009):

  "*Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig [...] überprüft werden können.*"
- Prohibition of electronic voting devices

Internet Voting Today

NORWAY

- Development of a new system (since 2009)
- Goals
  - Follow "Guidelines on Transparency of E-Enabled Elections" (Council of Europe, 2010)
  - Collaboration with research community
  - Learn from mistakes of other countries
- Communal and regional elections in 2011

Internet Voting Today

in research

Internet Voting Today

- >200 technical research papers (since 1988)
- Many non-technical research papers
- >6 specialized international conferences
  - VoteID
  - EVT/WOTE
  - EVOTE
  - REVOTE
  - SecVote
  - Swiss E-Voting Workshop

Internet Voting Today

- Existing implementations
  - Helios (USA, Belgium)
  - Civitas (USA)
  - Scantegrity II (USA)
  - Prêt-à-Voter (Luxembourg, UK)
  - Baloti.ch (Switzerland)
- Correctness of result is publicly verifiable
- Little experience with real elections

Internet Voting Today

- Standard cryptography
  - encryption
  - digital signatures
- Advanced cryptography
  - homomorphic tallying
  - blind signatures
  - secret sharing
  - threshold cryptosystems
  - mix networks
  - zero-knowledge proofs

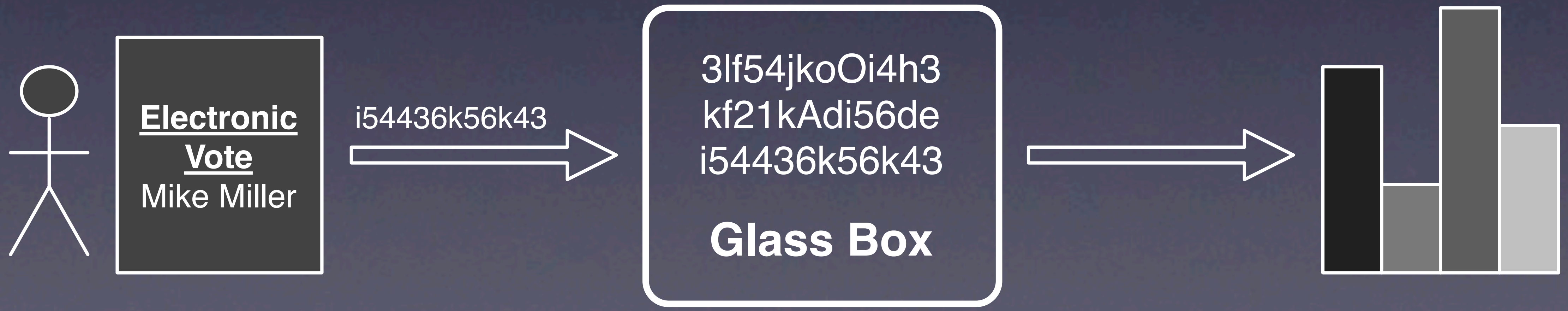
Internet Voting Today

- The “perfect” system is still missing
- Open problems
  - secure platform
  - Vote buying and coercion
  - Long-time privacy
  - Usability of complex cryptography
- Many cryptographers are against Internet voting

Verifiability

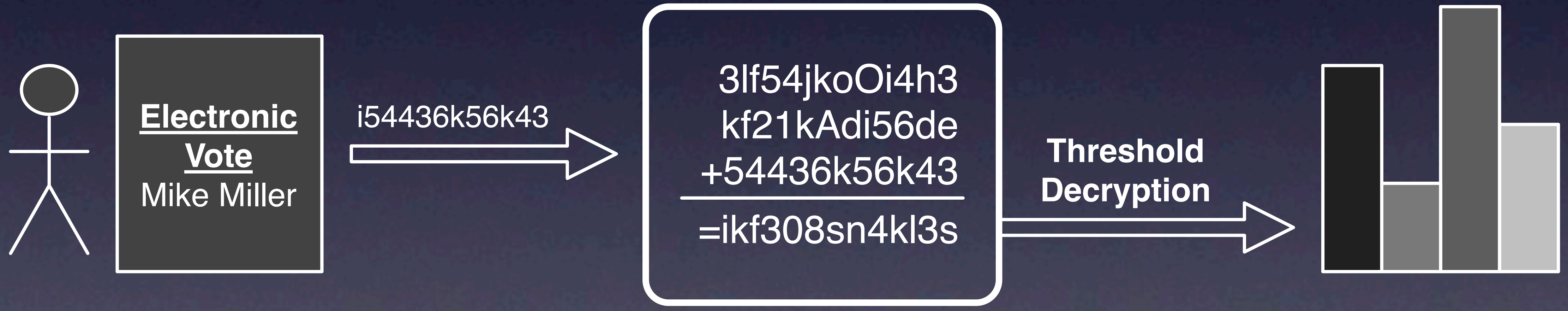
Verifiability

- Verifiability is achieved by using a “transparent ballot box”
  - Encrypted votes are posted to a public bulletin board
  - All computations of the election administration are documented on the bulletin board
  - ... and can be verified



Internet Voting Today

- Example: Homomorphic tallying
  - votes remain encrypted
  - sum of encrypted votes = encrypted sum of votes



  - multiple parties are involved in the decryption
  - zero-knowledge proofs are needed to prove validity of votes

Verifiability

- Verifiability ...
  - implies the correctness of the result
  - minimizes the necessary trust towards the authorities
  - makes the system more trustworthy
  - simplifies disputes
  - is postulated by the research community

Conclusion

Conclusion

- Today’s Internet voting systems are black boxes
  - the election result is not verifiable
  - authorities need to be trusted
- Research postulates verifiable Internet voting system
  - the election data is public (only keys remain secret)
  - all calculations can be verified (by anyone)
  - several cryptographic approaches exist

Questions?

(more information available at http://e-voting.bfh.ch)