Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

CoSin 2018: E-Voting

17. Juni 2018

Eric Dubuis

E-Voting @ BFH: Wer sind wir?

- Seit 10 Jahren betreiben wir Forschung zum Thema e-Voting
- Eine Grundannahme:

  Wir haben es mit dem stärkst möglichen Angreifer zu tun

- NB: Seriöse e-Voting-Forschung gibt es seit rund 30 Jahren

Vor 10 Jahren ...

- ... gingen wir zur Bundeskanzlei
- ... stellten Fragen

- ... sagten klipp und klar, dass «ihr» e-Voting nicht so nicht betreiben könnt:
  - Blackbox-System
  - «Security by Obscurity»

- Der Begriff «Verifikation» (im Zusammenhang e-Voting) war unbekannt

Wenn schon e-Voting, dann

- ... fordern wir die «bestmögliche» Lösung

Um dies zu unterstreichen

- haben wir geforscht (viele Publikationen)
- verifizierbare e-Voting-Systeme gebaut (z.B. UniVote)

Wunschvorstellung: Das e-Voting-System kann von Google oder der NSA betrieben werden...

Konkret (weg von der Träumerei) …

- Mitwirkung bei der gesetzlichen Bestimmung von e-Voting «Verordnung der BK über die elektronische Stimmabgabe (VEleS)»

  ➔ konkret: beim technischen Anhang

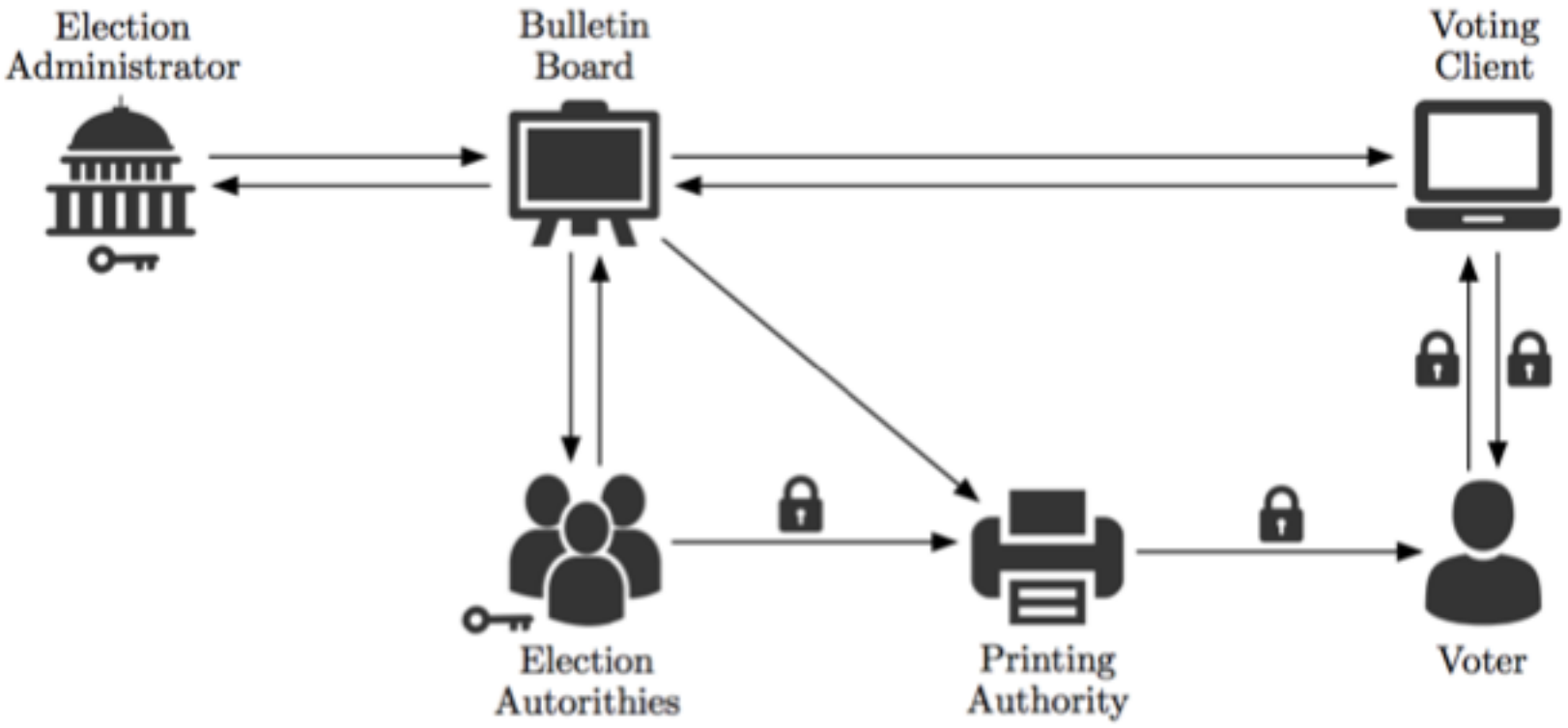
- Verfassung der CHVote-Spezifikation https://eprint.iacr.org/2017/325.pdf

- Mandat von der Post AG

CHVote-Spezifikation

- präzise Spezifikation eines e-Voting-Systems
- E2E-Verschlüsselung
- verifizierbares Mixnet
- *oblivious transfer*-Ansatz für *private information retrieval* (PIR)
- Postkanal zu Zustellung von Credentials und Codes
- individuelle Verifikation
- universelle Verifikation

CHVote: Übersicht



CHVote-Spezifikation: Vertrauensannahmen

- Druckerei
- *Privacy* der Voter-Plattform
- Mindestens eine der Kontrollkomponenten

Umkehrung: Ein Angreifer kann beliebige «andere» Komponente beherrschen (HW, Microcode, Firmware, OS, Libs, Tools, Applikation), auch in Kombination

➔ *kann nicht verhindert werden*

➔ *würde aber entdeckt*

Was ich mir wünsche, ist ...

- ... ein kompetenter fachlicher Diskurs

Und ...

- Forderung der Offenlegung der Spezifikation
- (Optional): Forderung der Offenlegung des Quellcodes

- Forderung der Offenlegung der Spezifikation der Verifikationssoftware
- Partizipation an der universellen Verifikation
- Forderung, eine Kontrollkomponente zu machen

Danke

Prof. Dr. Eric Dubuis
Berner Fachhochschule – RISIS
E-Voting Group
https://e-voting.bfh.ch
eric.dubuis@bfh.ch