Internet Voting with Trusted Hardware

Rolf Haenni & Reto E. Koenig

Research Institute for Security in the Information Society (RISIS)
Bern University of Applied Sciences (BFH)

Verifiable Voting Schemes Workshop

University of Luxembourg
March 21–22, 2013

Outline

Motivation

Secure Platform Problem

Internet Voting with Trusted Hardware

Discussion

Conclusion

Outline

Internet Voting

- The Internet is untrustworthy
- Voters are untrustworthy
- Voting authorities are (possibly) untrustworthy
- The voters' personal computers are untrustworthy

Internet Voting

- The Internet is untrustworthy
- Voters are untrustworthy
- Voting authorities are (possibly) untrustworthy
- The voters' personal computers are untrustworthy

Secure platform problem

Internet Voting in Switzerland

- Direct democracy
- Many referendums and popular initiatives
- Usually four voting periods/year
- On federal, cantonal, communal level
- Plus elections every 4 years
- Full voting rights for expatriates
- 3 different Internet voting systems in use
- 10 years experience

Internet Voting in Switzerland

- Direct democracy
- Many referendums and popular initiatives
- Usually four voting periods/year
- On federal, cantonal, communal level
- Plus elections every 4 years
- Full voting rights for expatriates
- 3 different Internet voting systems in use
- 10 years experience

Secure platform problem unsolved

Verifiable Internet Voting in Switzerland

- Baloti: Voting platform for migrants (2009–2011)
- UniVote: Student board elections (since 2012)
  - → University of Berne (today at 12am)
  - → Berne University of Applied Sciences (next week)
  - → University of Zurich (next month)
  - → University of Basel
- PrimeVote: Internet voting for shareholder meetings

Verifiable Internet Voting in Switzerland

- Baloti: Voting platform for migrants (2009–2011)
- UniVote: Student board elections (since 2012)
  - → University of Berne (today at 12am)
  - → Berne University of Applied Sciences (next week)
  - → University of Zurich (next month)
  - → University of Basel
- PrimeVote: Internet voting for shareholder meetings

Secure platform problem unsolved

Outline

Secure Platform Problem

- Theory: Voters have access to reliable computers that . . .
  - → display correct election information
  - → encode and encrypt vote (as intended)
  - → do other cryptographic computations (signature, ZKP, . . .)

Secure Platform Problem

- Theory: Voters have access to reliable computers that ...
  - → display correct election information
  - → encode and encrypt vote (as intended)
  - → do other cryptographic computations (signature, ZKP, ...)
- Practice: Voters use unreliable computers
  - → Viruses, man-in-the-browser, Trojans, spyware, keylogger, ...
  - → Estimated 1.4 millions new Windows malware in 2012
  - → Eurograbber: estimated 36 millions Euros stolen

Solution 1

Making the platform secure:

- Anti-malware software, firewall, etc.
- Booting from trustworthy media (CD, USB stick, etc.)
- Trusted computing

Solution 1

Making the platform secure:

- Anti-malware software, firewall, etc.
- Booting from trustworthy media (CD, USB stick, etc.)
- Trusted computing
- Limitations:
  - → Outdated anti-malware software
  - → System incompatibilities
  - → Booting not supported
  - → User acceptance

Solution 2

Using an auxiliary trusted channel:

- Code voting
- Verifications codes
- Finalization codes
- Postal mail (SMS, telephone)

Solution 2

Using an auxiliary trusted channel:

- Code voting
- Verifications codes
- Finalization codes
- Postal mail (SMS, telephone)
- Limitations:
  - → Repetitive costs for every election
  - → Slow
  - → Usability
  - → Secure printing
  - → Reliability of auxiliary channel

Solution 3

Challenge insecure platform with indistinguishable test ballots

- Voter-initiated auditing (Benaloh, 2007)
- Implemented in Helios
- Test elections indistinguishable from real ones

Solution 3

Challenge insecure platform with indistinguishable test ballots

- Voter-initiated auditing (Benaloh, 2007)
- Implemented in Helios
- Test elections indistinguishable from real ones
- Limitations:
  - → Integrity of real ballot not guaranteed
  - → Auditing on different platform
  - → Usability
  - → Confusing for voters

Outline

Requirements

- Easy to use (even for complex elections)
- Simple (no system updates)
- Efficient (cryptographic computations)
- Flexible enough to work with different voting protocols
- Offline
- Reliable
- Low-priced

General Concept

Demo

- Simulation on smartphones
- Bachelor thesis (von Bergen, Pellegrini, 2012)

Personal Voting Card

- Personal smartcard
- Provides an authentication mechanism
- Stores the voter's voting credentials
- Generates credentials on board
- Cryptographic computations involving the credentials

Voting Device

- Impersonal (e.g., one per household)
- Card reader slot
- Small textual display
- Keypad (PIN, scrolling)
- Optical scanner to read 2D-barcodes
- Software-closed
- Tamper-resistant
- Offline
- Cryptographic computations: vote encryption, ZKP, ...

Voting Platform

- Web application (with standard security measures)
- No login process
- No secret data
- Maximal usability
- Display 2D-barcodes containing . . .
  - → signed election description
  - → signed options
  - → other cryptographic elements (depending on protocol in use)

Outline

Security

- The voter's untrustworthy personal device ...
  - → is no longer the communication channel endpoint
  - → broadcasts over an optical channel
  - → does not learn the voter's choice

Security

- The voter's untrustworthy personal device ...
  - → is no longer the communication channel endpoint
  - → broadcasts over an optical channel
  - → does not learn the voter's choice **Vote Secrecy ✓**

Security

- The voter's untrustworthy personal device ...
  - → is no longer the communication channel endpoint
  - → broadcasts over an optical channel
  - → does not learn the voter's choice

  Vote Secrecy ✓
- The trustworthy voting device ...
  - → displays the official election information
  - → lets the voter confirm the choice
  - → generates and encrypts the vote

Security

- The voter's untrustworthy personal device ...
  - → is no longer the communication channel endpoint
  - → broadcasts over an optical channel
  - → does not learn the voter's choice **Vote Secrecy ✓**
- The trustworthy voting device ...
  - → displays the official election information
  - → lets the voter confirm the choice
  - → generates and encrypts the vote **Vote Integrity ✓**

Security

- The voter's untrustworthy personal device ...
  - → is no longer the communication channel endpoint
  - → broadcasts over an optical channel
  - → does not learn the voter's choice — **Vote Secrecy** ✓
- The trustworthy voting device ...
  - → displays the official election information
  - → lets the voter confirm the choice
  - → generates and encrypts the vote — **Vote Integrity** ✓
  - → performs all cryptographic operations
  - → does not generate a receipt — **Receipt-Freeness** ✓

Costs

- Design, production, distribution is expensive
- Costs can be shared among multiple users
- Use for other application (online banking)
- Reduced/modest costs to run the voting web application
- Switzerland: costs per vote reasonably small

Example: Cronto Device

Outline

Conclusion

- Protects vote secrecy and vote integrity
- Compromise between usability, simplicity, costs
- Vote preparation on all platforms (even on paper)
- Compatible with various cryptographic voting protocols
- May help to prevent vote buying / coercion
- Possibly applicable to other applications

Reference

Rolf Haenni & Reto E. Koenig

Voting over the Internet on an Insecure Platform.

Design, Development, and Use of Secure Electronic Voting Systems

IGI Global, 2013 (to appear)