Dagstuhl Seminar

Secure Internet Voting on an Untrusted Platform

July 12th, 2011

Rolf Haenni

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

Who are We?

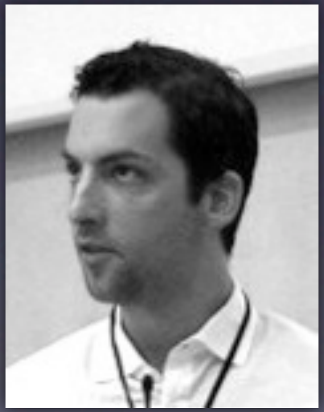
- E-voting research group since 2007
- 3 professors, 2 PhD students, 3 assistants
- Activities
  - Vote-ID’07, EVOTE’10, ISSA’10, FC’11, IFIP’11, CeDem’11, EVT/WOTE’11, ICEGOV’11
  - Swiss E-Voting Workshop 2009 & 2010
  - Baloti.ch (e-voting platform for immigrants living in Switzerland)

Eric Dubuis

Rolf Haenni

Stephan Fischli

Reto Koenig


Oliver Spycher

José Beuchat

Secure Platform Problem

Internet Voting

- The Internet is untrustworthy

Internet Voting

- The Internet is untrustworthy
- Voters are untrustworthy

Internet Voting

- The Internet is untrustworthy
- Voters are untrustworthy
- Voting authorities are (possibly) untrustworthy

Internet Voting

- The Internet is untrustworthy
- Voters are untrustworthy
- Voting authorities are (possibly) untrustworthy
- The voters’ personal devices are untrustworthy

Secure Platform Problem

Secure Platform Problem

- Approach 1: Making the platform secure
  - Booting from trustworthy media (CD, USB stick, etc.)

Secure Platform Problem

- Approach 1: Making the platform secure
  - Booting from trustworthy media (CD, USB stick, etc.)
- Approach 2: Using a secure channel
  - Code voting (PGD, etc.)

Secure Platform Problem

- Approach 1: Making the platform secure
  - Booting from trustworthy media (CD, USB stick, etc.)
- Approach 2: Using a secure channel
  - Code voting (PGD, etc.)
- Approach 3: Distributing a secure platform
  - Trustworthy voting device

Code Voting

- Pros
  - Infrastructure exists (postal service)
  - No initial costs
- Cons
  - Repetitive costs for every election
  - Slow
  - Not very user friendly (entering the codes)
  - Secure printing problem
  - Reliable? Secure?

Secure Voting Device

- Pros
  - No repetitive costs for every election
  - Experience in related applications (online banking)
  - Compatible with existing protocols
  - Useful for storing/accessing personal credentials
- Cons
  - High initial costs (development, production, distribution)
  - Support required (helpline)
  - Trustworthy?

Secure Voting Device

General Idea

General Idea

- The voter’s untrustworthy personal device ...
  - is no longer the endpoint of the communication channel
  - does not learn anything about the voter’s choice

General Idea

- The voter’s untrustworthy personal device ...
  - is no longer the endpoint of the communication channel
  - does not learn anything about the voter’s choice
- The trustworthy voting device ...
  - lets the voter prepare/confirm the choice
  - generates the electronic ballot
  - performs all the necessary crypto
  - does not generate a receipt

Requirements

- Easy to use (even for complex elections)
- Low-priced
- Simple (no system updates)
- Reliable
- Efficient (crypto primitives)
- Mobile
- Compatible

Components

Components

- Voting card
  - personal smartcard
  - provides an authentication mechanism
  - stores the voter’s voting credentials
  - performs the crypto involving the credentials

Components

- Voting card
  - personal smartcard
  - provides an authentication mechanism
  - stores the voter's voting credentials
  - performs the crypto involving the credentials
- Voting device
  - impersonal (e.g., one per household)
  - has a small display and a few buttons
  - has an optical scanner to read 2D-barcodes

Discussion

- Compromise between usability, simplicity, costs

Discussion

- Compromise between usability, simplicity, costs
- Vote preparation on all platforms (even on paper)

Discussion

- Compromise between usability, simplicity, costs
- Vote preparation on all platforms (even on paper)
- Compatible with various e-voting protocols

Discussion

- Compromise between usability, simplicity, costs
- Vote preparation on all platforms (even on paper)
- Compatible with various e-voting protocols
- May help to prevent vote buying / coercion

Discussion

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

Questions & Discussion

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