



E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
SCV

E-voting over Untrusted Devices

Mirek Kutyłowski

Wrocław University of Technology

Dagstuhl, 20.06.2008



Types of e-voting

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting
Problem setting
requirements
E2E systems

Problems with
voting
paper based
hardware

Solution
ideas
SCV

Voting machines

replacing ballot box and paper ballots with an electronic device

Paper based

clever procedures and ballot designs so that cheating becomes impossible

Remote voting

voting procedures executed by the voters remotely with their electronic devices (PC, phones,...).



Requirements

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

Most common requirements

- 1 only legitimate voters can cast votes
- 2 no double voting - no voter can vote twice
- 3 correctness of results - the outcome corresponds to the votes cast
- 4 anonymity - nobody can deduce any information about the choice of a particular voter (except for information directly revealed by election results)
- 5 no vote selling - the voter cannot prove how he voted,
- 6 *verifiability* - a voter (or an observer) can check the results



End-to-end voting systems

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements

E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

Assumption: no component can be trusted

in particular:

- voting authority
- tallying authorities
- voters
- machines

E2E system:

nevertheless, it should be secure

no E2E system has been deployed yet (including non-electronic ones)



Problems with paper based voting

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

Some major concerns

- anonymity issues
- vote selling
- manipulating ballots (making them invalid,...)

Limitations

manual procedures cannot be expanded too much for usability reasons



Necessity of hardware

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

cases

efficiency - Japan, Hamburg,...

safety of ballot box - Brasil, India, ...

safety of voters - ...

mobility of voters - Poland, USA



Special purpose equipment

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting
Problem setting
requirements
E2E systems

Problems with
voting
paper based
hardware

Solution
ideas
scv

Economic problems

- single purpose equipment
- consequences of discovering flaws (replacement?)
- authentication

Technological problems

- verification versus proprietary, secret layout
- imperfect randomness
- malicious designs (kleptography)



General Idea

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting
Problem setting
requirements
E2E systems

Problems with
voting
paper based
hardware

Solution
ideas
scv

limited knowledge

- there is some knowledge physically away from hardware
- without this knowledge a device used for voting cannot see the voter's preference
- computing device only as an unconscious calculator and communication device

Audit on protocol level

a device can cheat but the protocol assures that it can be detected with a reasonable probability



E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

Scratch, Click & Vote

joint work with Filip Zagórski



Actors

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

- 1 Election Authority - responsible for creating ballots
- 2 Proxy - responsible for creating coding cards
- 3 PC
- 4 voter



A ballot

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

Candidate	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
2 Jerry				
3 Edgar				
0 Ervin				
1 Donald				
S_i				

- the list of the candidates shifted circularly by x positions, x chosen at random,
- ballot serial number S_i ,
- *confirmation tokens*: A, B, C, D – one per column, prepared in a special way.



A coding card

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

	n	Y	n	n
	n	Y	n	n
	Y	n	n	n
	n	n	n	Y
	S_r			



Complete ballot+voting card

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

<i>Candidate</i>	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
S_l	S_r			



Voting for Erwin

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

■			
		■	
■			
	■		

S_r



Transformation by a proxy

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

		×	×
×			×
	×	×	×
×		×	



Submitting ballot

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

Procedure

- 1 Proxy obtains a blind signature (BS) of EA under each ballot column.
- 2 The voter enters S_i , then Proxy unblinds the signature, and sends ballot columns with S_i to EA.
- 3 The voter gets one column signed as a receipt via oblivious transfer.



Receipt

E-voting over
Untrusted
Devices

Mirek
Kutyłowski

E-voting

Problem setting
requirements
E2E systems

Problems with
voting

paper based
hardware

Solution

ideas
scv

Contents of a receipt

- $T \in \{A, B, C, D\}$ a value of a confirmation token,
- y - a ballot column,
- t such that $T = \text{sign}_{EA}(t, S_I)$, such a t is called a pre-token of T .