

# End-to-End E-voting Systems

Filip Zagórski

Institute of Mathematics and Computer Science  
Wrocław University of Technology

EFPE

Międzyzdroje, 4-6 VI 2008

# E-voting

- ▶ e-voting:
  - ▶ voting machines at polling places (evoting)
  - ▶ voting over the Internet (ivoting, remote voting)

# “Classical” approach

- ▶ For the last 20 years tens (hundreds?) evoting schemes have been proposed
- ▶ Motto: Evoting is as easy as building any other electronic system. We have a lot of cryptographic tools (digital signatures, RSA, ElGamal, blind signatures etc.) let's put them together!
- ▶ Model: Voter and her PC against Election Authority
- ▶ people were mainly focused on making schemes more efficient

# “Classical” approach

## Typical solution

- step 1** a voter downloads a voting application from a special server (or visits election website),
- step 2** using the program (or applet), the voter prepares a ballot a resulting ciphertext that must be decrypted by many tallying authorities,
- step 3** the voter sends a signed ballot to an appropriate authority.

## Problem with “classical” approach

- ▶ a voter and her voting terminal are the same actor in the system
- ▶ quotes from one of the scheme descriptions:
  - ▶ “Voter  $V_i$  includes non-interactive proofs of knowledge of  $\sigma_i$ ”
  - ▶ “Voter signs message  $m$  and sends it to...”

## “Classical” approach - vote selling

- step 1 download and install an appropriate tracing program from a server located at *Voting Islands*,
- step 2 prepare a ballot and submit it while the tracing program is activated,
- step 3 the tracing program sends a message to Voting Islands
- step 4 the voter gets digital cash or some access codes
- step 5 the voter de installs the tracing program.

# “Classical” approach - malware attack

- ▶ Even if a voter is honest, her PC can be infected by a virus with similar functionality.
- ▶ Even if a voter is honest and secures her computer, voting program may contain kleptographic code.
- ▶ Is voting at polling stations more reliable?  
Of course not - the same approach in system design was used (see “California report” - [www.sos.ca.gov/elections/elections\\_vsr.htm](http://www.sos.ca.gov/elections/elections_vsr.htm))

[www.DagstuhlAccord.org](http://www.DagstuhlAccord.org)



# E2E - End To End Voting Schemes

E2E “definition” ([www.DagstuhlAccord.org](http://www.DagstuhlAccord.org))

- ▶ allow each voter to ensure that his or her vote cast in the booth is recorded correctly

# E2E - End To End Voting Schemes

E2E “definition” ([www.DagstuhlAccord.org](http://www.DagstuhlAccord.org))

- ▶ allow each voter to ensure that his or her vote cast in the booth is recorded correctly
- ▶ allow anyone to verify that all such recorded votes are included in the final tally correctly

# E2E - End To End Voting Schemes

E2E “definition” ([www.DagstuhlAccord.org](http://www.DagstuhlAccord.org))

- ▶ allow each voter to ensure that his or her vote cast in the booth is recorded correctly
- ▶ allow anyone to verify that all such recorded votes are included in the final tally correctly
- ▶ provide privacy of votes

# E2E - End To End Voting Schemes

E2E “definition” ([www.DagstuhlAccord.org](http://www.DagstuhlAccord.org))

- ▶ allow each voter to ensure that his or her vote cast in the booth is recorded correctly
- ▶ allow anyone to verify that all such recorded votes are included in the final tally correctly
- ▶ provide privacy of votes
- ▶ do not rely on trust in particular persons, manual processes, devices or software

# E2E - End to end verifiability

- ▶ E2E let us verify:
  - ▶ cast as intended
  - ▶ recorded as cast
  - ▶ counted as recorded
- ▶ Security verification is outside the system!

# E2E voting schemes

- ▶ E-voting examples (at polling stations)
  - ▶ Punchscan (Chaum) 2005
  - ▶ Prêt à Voter (P. Y. Ryan) 2005
  - ▶ ThreeBallot, VAV, TWIN (Rivest) 2006
  - ▶ Scantegrity (Chaum) 2007
  - ▶ Scantegrity II (Chaum) 2008
- ▶ I-voting example
  - ▶ Scratch, Click & Vote (Kutyłowski, Zagórski) very soon

# Voter vs Terminal part I

- ▶ If a machine has the same knowledge as a voter, one cannot do nothing:
  - ▶ machine knows exactly how voter voted
  - ▶ machine can change our choice
- ▶ Solution: voter obtains additional information by an independent channel – “voting card” (paper is back?!) prepared by an Election Authority

## Voter vs Terminal part II

- ▶ Machine cannot change an “order” of a Voter – voter obtains a receipt, which can be used to detect machine’s misbehaviour.
- ▶ But at the same time, “voting card” and a receipt cannot be used to prove voter’s choice
- ▶ Achieving these two properties is the hardest part in the system design.

# Voter vs Election Authority

- ▶ Voter obtains voting card (ballot) from Election Authority
- ▶ How does voter know if her voting card is correctly encoded? **Pre-election Audit**
- ▶ How can one protect voter's privacy?  
**Use ballot box** (real or electronic one - "proxy")

# Ballot (FourBallot)

- ▶ Voter obtains a voting card

	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
candidate 3				
candidate 4				
candidate 1				
candidate 2				

- ▶ list of candidates is shifted
- ▶ shift is encoded in *A*, *B*, *C*, *D* (“serial numbers”)

# Arming a card

- ▶ Voter “arms” a card

	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
candidate 3	×		×	
candidate 4		×	×	
candidate 1	×	×		
candidate 2			×	×

- ▶ Each candidate obtains 2 ×-marks

# Voter's choice

- ▶ Voter chooses *Candidate 4*

	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
candidate 3	×		×	
candidate 4		×	×	×
candidate 1	×	×		
candidate 2			×	×

- ▶ *Candidate 4* gets another ×-mark

# Scanning

- ▶ Each ballot is scanned (enters the system)

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
×		×	
	×	×	×
×	×		
		×	×

# Receipt

- ▶ Voter takes home one of the columns as a receipt

C
×
×
×

- ▶ System does not know which ballot was taken – system has to count all votes!
- ▶ Single column does not reveal voter's choice

# Coding card

- ▶ Voter obtains a *voting card* from Election Authority
- ▶ Voter obtains many *coding card* from “Proxy”
- ▶ Voter lays them side by side

Candidate	A	B	C	D
2 Jerry				
3 Edgar				
0 Ervin				
1 Donald				
$S_l$				

n	Y	n	n
n	Y	n	n
Y	n	n	n
n	n	n	Y
$S_r$			

Candidate	A	B	C	D
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
$S_l$	$S_r$			

# Casting a vote

- ▶ Voter clicks on the screen on boxes which correspond to  $Y$  next to his candidate and to  $n$ 's

Candidate	A	B	C	D
2 Jerry	n	Y	n	n
3 Edgar	n	Y	n	n
0 Ervin	Y	n	n	n
1 Donald	n	n	n	Y
$S_i$	$S_r$			

■			
		■	
■			
	■		

$S_r$

		×	×
×			×
	×	×	×
×		×	

$S_i$

- ▶ Proxy transforms it into ballot (Proxy does not know shift used)
- ▶ PC cannot change voter's choice (with high probability)

# E-voting

- ▶ voting machines at polling places (evoting)
  - ▶ voter's identification – traditional
  - ▶ voting booth – one can assure voter's privacy
  - ▶ ballot box – easy way to anonymize votes
  - ▶ receipt freeness – easy to force a voter to i.e. shred a voting card
- ▶ voting over the Internet (ivoting, remote voting)
  - ▶ voter's identification – digital signature
  - ▶ “proxy” – server operated by each party or watch-dog organizations

# E2E voting schemes

- ▶ E-voting examples (at polling stations)
  - ▶ Punchscan (Chaum) 2005
  - ▶ Prêt à Voter (P. Y. Ryan) 2005
  - ▶ ThreeBallot, VAV, TWIN (Rivest) 2006
  - ▶ Scantegrity (Chaum) 2007
  - ▶ Scantegrity II (Chaum) 2008
- ▶ I-voting example
  - ▶ Scratch, Click & Vote (Kutyłowski, Zagórski) very soon

- ▶ Thank you for your attention