Remotegrity

Design and Use of an E2E Verifiable Remote Voting System

David Chaum, Rick Carback,
Jeremy Clark, Aleks Essex,
Poorvi Vora, Filip Zagórski

Background

- 2009 - The City of Takoma Park, MD, Municipal Election – First voter verifiable system used to elect government officials (Scantegrity II).
- 2011 - Scantegrity II used again.
  - Remotegrity - mailed form enabled online voting (optional).

Absentee voting - problems

- voter does not know how her/his vote will be counted,
- voter does not even know if her vote reached EA,
- voter authentication,
- privacy,
- vote buying/coercion.

Voting over the Internet – more problems

If a voter's PC has the same knowledge as a voter:

- ballot secrecy (malware) Estonia, Norway, D.C., Switzerland, Helios, . . .
- (most cases) integrity (what happens when client/server side is hacked): Estonia, D.C., Switzerland, Helios, . . .

Remotegrity - design goals

A method for remote voting based on ballots mailed to voters and cast over the Internet that provides strong protection against:

- client-side malware,
- malfeasance by election officials,
- attacks over the Internet (but not DDOS).

As most of E2E schemes these are detection mechanisms not prevention mechanisms... but has failover modes.

Election package

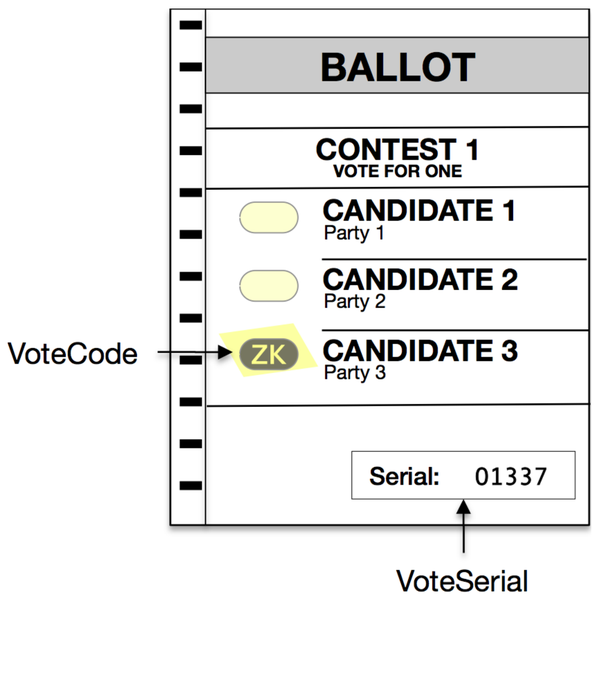
- a Scantegrity I/II or eg. Pret a Voter ballot,
- an authorization card,
- inner return envelope,
- outer postal return envelope.

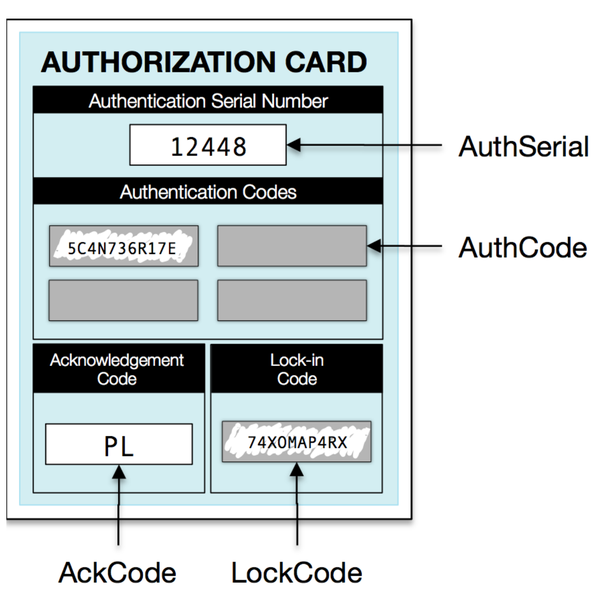
Ballot properties

- Computer/malware does not learn voter's choice.
- Computer/malware cannot modify voter's choice.
- Voter can check if her vote is included in a tally.

Ballot properties: Scantegrity II

- Better dispute resolution.





Authorization card properties

- Malware cannot cast ballot for a voter.
- ***New:*** Election authorities cannot cast ballot for a voter (the voter choice of scratch-off is a kind of oblivious transfer).
- ***New:*** Voter has a physical proof in case of malfeasance.

Ballot casting

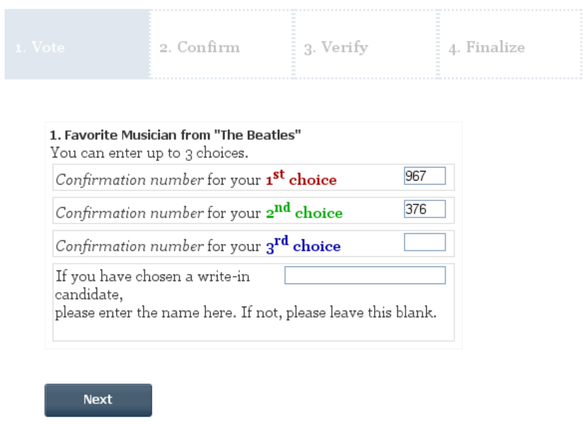


Figure: Step 1. A voter enters confirmation codes from a ballot.

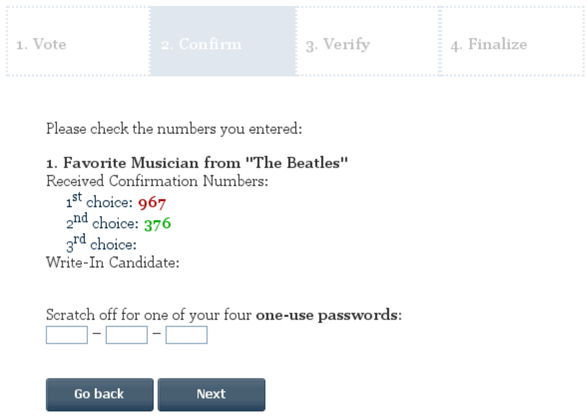


Figure: Step 2. A voter checks the codes and enters one time password.

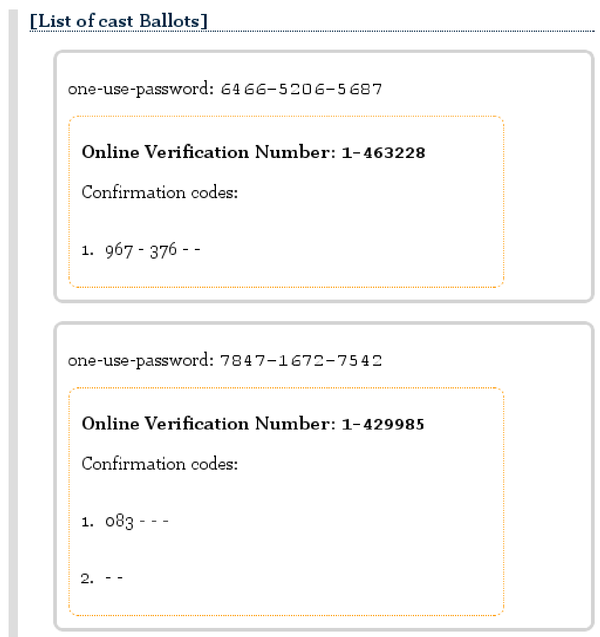


Figure: Step 3 (Optional): A voter checks if codes are posted correctly, verifies AckCode and AuthCode

Security – usability tradeoffs

- I want to "click" on my candidate...
  then your computer/malware knows who you vote for.
- I don't want to revisit election webpage... then you don't know if your ballot is **recorded as cast**.

What can malware do?

- does not learn how you vote
- can send different codes (a voter can discover that by checking Bulletin Board)

What can hacker do (server side)?

- Cannot change votes already posted (entries are signed by an offline server).
- Cannot discard new ballots received – voters detect that by checking Bulletin Board - if the correct serial of the Authentication Card is posted on BB, the voter knows it reached Election Officials – connection between one use passwords and serials is stored on offline machine.
- Can DDOS.

	Software Independence	Voter Verifiable Tally	Ballot Secrecy	Coercion Resistant	Malware Resistant	DOS-Resistant	Blank	Phishing Protection	MITM Protection	Recover from Lost Ballot	Prevent Insider Attack	Responsive	Prevents Credential Theft	Blank
Remotegrity	●	●	●	●	●	○	X	○	○	●	●	●	●	X
Code Voting	●	●	●		●		X	○		○	○	●		X
Vote-by-Mail	●		○		●	●	X	●	○					X
Proxy Voting	●				●	●	X	●	●		○	●	●	X
Online Voting			○				X			●		●		X
Coercion-Resistant		●	●	●			X			○	●	●	●	X

Table: A Comparison of Absentee Voting Schemes. ⋆ - there is a coercion-resistant version of the Remotegrity system. It differs with registration procedures.

More

- Scantegrity.org Blog :: Remotegrity FAQ
  `www.scantegrity.org/blog/`

Our work builds on the considerable work of the Scantegrity research team.
This research was funded in part by NSF Awards 0937267 and 1137973, including a Research Enhancement for Undergraduates (REU).
This work is partially supported by Polish NCN grant N N206 369839 and FNP programme MISTRZ.

The system was implemented and operated by Essevo Ltd. `www.essevo.com`