A Practical Web-Voting System

Andrea Pasquinucci
UCCI.IT
A Web Voting System

- Threat Scenario:
  - Analysis
  - Requirements
  - Goals
- Usability
- Protocol
- Cryptography
- Implementation
- Demo online at http://eballot.ucci.it/
What Does It Implies?

- Voters can express their vote from anywhere:
  - PC at home
  - PC at work
  - PC at kiosk
  - Smartphone
  - ...

=> DELOCALIZATION

- Easier to participate
- More difficult to control
Delocalization Problems

- Common to ALL delocalized voting systems
  - Mail
  - Phone
  - Fax
  - Web

- Coercion
- Vote-Selling

- No valid countermeasures
Trust Problems

- Traditional voting systems have intrinsic human control features
- Web-Voting (and E-Voting) requires Trust in IT by
  - Voters
  - Electoral committee
  - Representatives of the competing parties

- Nobody really Trusts a computer!

- Alternative control measures must be in place
- NB: Votes must be anonymous and correctly counted
Independent Control

Human

Voter

Check Votes

Web Server

Votes DB

Results

IT
Simplest Solution

- Give Voter an **Anonymous Vote Receipt**
- Publish match Receipt <=> Votes
- Voter can:
  - Check if her own vote is counted correctly
  - Check if sum of votes is correct

- Receipt can make it easier to sell votes, but this is possible and easy anyway!
Thank You

Scientific Articles and Demo on-line at:

http://eballot.ucci.it/

Andrea Pasquinucci

pasquinucci-At-ucci.it     www.ucci.it
Copyright © Andrea Pasquinucci

License Creative Commons by-nc-nd 3.0:
Attribution, non commercial, no derivative works
http://creativecommons.org/licenses/by-nc-nd/3.0/