FACULTY OF SCIENCE

Bart Jacobs

Voting in the Netherlands Revisited

Radboud University Nijmegen

Contents

I. Background

Who is this guy?

- Professor in computer security, at Nijmegen & Eindhoven
- Focus not on functionality but on misuse
- Apart from academic abstract nonsense, involved in e-government / identity management, like biometric passports & voting
- Occasional role in media
- Author of online book *De Menselijke Maat in ICT*, see `www.cs.ru.nl/B.Jacobs/MM`

Own involvement in voting

- For internet voting in EU-'04: advisor & contractor for vote counting software
- Auditor for regional waterboard elections (RIES, '04) & independent counter ('04, '06)
- Author of scientific papers about this
- Invited lectures for Election Council (*Kiesraad*, 4/'05), civil servants, colleagues
- Member of committee *Korthals Altes*

Disclaimer: no crypto, but software person

Voting machines in NL, I

Nedap

Sdu

Voting machines in NL, II

- Introduced since early 90s; early 2006 used almost everywhere
- Votes stored in digital memory; internal mechanics is secret
- US terminology: "Direct-Recording Electronic voting machine" (DRE)
- Evaluation is required, done by TNO; reports are secret (and also partly missing)
- No meaningful recounts possible.

The main concern . . .

"Let's see how my vote is counted" ©Automatisering Gids 2003.

Voting machines in NL, III

Advantages

- automatic processing of results: efficient and fast (especially for local organisers: municipalities)
- vote expression is unambiguous

Disadvantages

- Voter cannot verify that the vote is registered correctly
- Recount only possible on already processed votes

Back then . . .

- The introduction of these voting machines in NL since early 90s was uncontroversial
- Openness (of software) was not an issue at the time.
- Much trust in technology (and in the state!)
- By now we know better about the unreliability and vulnerability of software and networks
- International controversy since 2004 (esp. relevant in IRL) without much effect in NL, . . . *at first . . .*

II. Controversy

The trigger

- March 2006: municipal elections in NL
- City of Amsterdam uses voting machines (from Sdu) for the first time
- One citizen was shocked: ***Rop Gonggrijp***
- . . . and started a foundation:

"*wedonottrustvotingcomputers.nl*"

Foundation's main points

- Not "voting machines" but "voting computers"
- Voting computers (Nedap & Sdu) are not protected against manipulation—like eg. game computers are
- Voting results are not verifiable
- Paper copy of each vote required.

Foundation's approach

- Set up very informative webpage
- Exploit *freedom of information legislation* and put all results on the web
- Start effective media campaign & newsletter
- Gather knowledgeable volunteers
- Take legal actions against every government move.

BJ: sympathy with goals, but no direct involvement

Foundation's main stunt

- Purchase of two Nedaps:

- Legal, from left-over after municipal merger
- Including all software ("ISS") for running an election.

Nedap deconstruction

- Motorola M68000 processor
- Two removable memory chips (EPROM) with OS & vote counting software
- Removable flash memory for holding votes
- Software was reverse-engineered, and new software written for:
  - chess playing on Nedap
  - "false" counting

Killer events

- TV program *EenVandaag*, 4/10/'06, showing:
  - Easy manipulation of Nedap software
  - Sloppy storage of 500 Nedaps in R'dam
- Tempest: electromagnetic radiation
  - Vote can be read from dozens of meters
  - Tension with vote secrecy requirement
  - Basis for legal action by Foundation.

Foundation's direct impact

- Approval of Sdu's withdrawn before NL parliament elections of nov. '06
  - Nedap tempest within ad hoc limits
  - Paper voting returned to Amsterdam
- Two government committees:
  - **Looking back:** "Hermans", with report *Stemmachines, een verweesd dossier*, 4/07
  - **Looking forward:** "Korthals Altes", with report *Stemmen met vertrouwen*, 9/07.

III. Looking back

Looking back committee (Hermans), I

- Voting machine initiatives in 80s came from industry (Nedap, TNO), for higher accuracy
- Requirements for voting machines:
  - only in late 90s
  - no steering by ministry or election council
  - focus on safety, not security/transparancy
  - vote counting software never covered
- Security and reliability concerns (like in IRL) ignored in NL, both nationally and locally

Looking back committee (Hermans), II

- Election council too dependent on (loose cannon) software supplier ("*omhelzing*")
- About the ministry
  - lack of technical expertise
  - not in control: too dependent on external (commercial) parties
  - has ignored signals of concern
- TNO wrote requirements & had evaluation monopoly
- Local authorities only want convenience

Official reaction

- Humble acceptance of conclusions
- Shift of "voting" within ministry, to department with more technical expertise
  (from CZW to BPR)
- Immediate redrafting of requirements for voting machines
  - Foundation sees attempt to save Nedaps
- Await "looking forward" report.

IV. Looking forward

Paranoia?

- ***Paper ballots*** are a bad idea because voters leave fingerprints and governments have databases of fingerprints these days and can thus read individual votes
- ***Computer-based*** voting is a bad idea because government (intelligence) services are best at reading tempest signals, and can thus read individual votes

Paranoia!

- Those things don't happen in a civilised country like NL. We should assume a minimal level of trust.
- But NL should set an example, also for countries where such trust is maybe not justified!

Looking forward: who were involved

- FLTR: Barendrecht, Meesters, Korthals Altes (chair), Jacobs, van der Wel
- Active from jan. to sept. 2007.

Looking forward: what was done

- Formulate requirements / safeguards
- Perform threat analysis
  (threat = risk * impact on safequard)
- Decide on basic form (poll station); establish exceptions
- Compare options within poll station
  (tempest is issue on its own)
- Organisational matters
  (mostly ommitted)

Own emphasis here on technical angle

Requirements / safeguards

- transparancy
- verifiability
- integrity
- eligibility
- unicity
- vote secrecy
- vote freedom
- accessibility

- Not all can hold absolutely: balance needed
- Poll station gives most guarantees
- Exceptions for severely disabled (phone) & expatriats (internet)

On the far side of being wrong

- Imagine “vote pillar”, eg. in train station, with:
  - Voter recognition via (biometric) passport
  - Vote expression via touch screen
  - Electronic storage of vote
  - Transmission to central office at end
- Sounds cool & convenient . . .
- Two fundamental problems: device may
  - store ***link*** between voter and vote
  - store or count votes ***incorrectly***

Basic idea of committee

- Create separation between phases
  - *identification*
  - *vote expression*
  - *vote storage*

  with individual voter as only connection!
- ***Within*** these phases use ICT as much as you like, but ***not inbetween***.

Implementation: “voteprinter”

- Vote expression via touchscreen
- Device stores nothing, but only prints individual vote in human readable manner
- Voter checks correctness of print:
  - **OK**, then print is deposited in ballot box
  - **NOT OK**, voter may vote again
    (upon repeated errors device is replaced)
- In the end votes are counted automatically
  (using optical character recognition, OCR)

Advantages voteprinter

- Recounts are possible, manually if preferred
- Actual vote casting is physical act (deposit)
- Software faults are detectable, by voters
- After failures, device can be replaced without effect on already cast votes (no internal state)
- Device can present many possible elections: vote anywhere, nationwide
- Voteprinter is flexible, fancy pencil
- Voting proces is centered around the voter

Main disadvantage: tempest risk

- Uncomfortable situation:
  - Expertise secretive (esp. intelligence services)
  - No public, but secret (NATO), norms
  - High demands on environment
  - High cost & evaluation per item
- Pragmatic recommendation:
  - Best effort, affordable technical measures
  - Repressive measures (punishable)

Additional recommendations

- Internet voting:
  - Transparancy, verifiability, freedom & secrecy unsufficiently guaranteed
  - Incomparable with internet banking etc.
  - Research dust has not come down yet
  - At this stage only for expats
  - Knowledge & experience remains present
- Independent audit of every election:
  - Report within 3 days for election council
  - Within 3 months analysis & recommendations

Upon finishing the report

- Remaining (Nedap) voting machines are dropped
- Paper voting returns until new voteprinter is introduced

V. Conclusions

Main points

- Foundation won its case
- Powerful & knowledgeable grassroot movement against “wrong kind” of ICT
- Solution puts people at center
- Which sector is next? OV-chip, EPD, EKD, . . .

Thanks for your attention!