The issue ...

"Let's see how my vote is counted"

Is Remote-Voting far from Reliable?

Bart Jacobs

bart@cs.kun.nl http://www.cs.kun.nl/~bart.

Security of Systems (SoS),
Department of Computer Science
University of Nijmegen

Contents

I. Background Info

Topic

Concretely

- European Elections of June 2004 will allow “Remote Voting” or “*Kiezen op Afstand*” via ***internet*** and ***phone***
- Intended for expatriats, after registration

Abstractly

- New technology requires reconsideration of the essentials of voting
  (Similarly with electronic signatures, for instance)
- Risk identification

Who am I?

- Professor of Software Security and Correctness since 2002 (Inaugural speech in May 2003).
- Leader of a (top) security group of 12 researchers at Nijmegen University.
- Occasional role in discussions in the media on “security in society” topics:
  - bank cards
  - privacy
  - phone tapping
  - open source software
  - digital signatures
  - …

But I am not a legal expert!

What we do in Nijmegen

- Origins are in (Java) ***program verification***, with ***smart cards*** as main application area.

- Shift to ***software security*** in recent years
- Emphasis on technical work, but with open eye for influence from & impact on ***society***
- Emphasis on ***transparancy & openness***
- Occasional ***audit*** work—where we demand that our reports will be public

Involvement in remote-voting

- Professional interest in challenging & hot topic
- Writer of patent application in this area (september 2002, in EC & US)
- Member of external ***expert panel*** of BZK (august 2003)
- Non-commercial audit of webservice in voting trial (november 2003)
- Commercial assignment to build vote counting software (march 2004)

But: no detailed knowledge of entire system!

II. Voting Essentials

Requirements

Correctness

- Each valid vote should contribute precisely once to the final outcome.
- The result should be verifiable: recounts possible

Security

- ***Confidentiality***: votes should not be traceable—to prevent use of force and sale of votes
- ***Integrity***: the expressed vote should contribute (unchanged) to the outcome
- ***Availability***: vote intentions should be realisable

Different approaches

1. Traditional paper ballots
2. Voting machines (in voting stations)
3. Online voting systems

Paper ballots

Advantages

- Low-tech, transparent system
- Security lies in distributed character: large scale tampering is difficult, and easy to observe
- Vote counting happens in public
- Recount possible with original, unprocessed data

Disadvantages

- No automatic processing: labour-intensive and slow
- Vote expressions may be ambiguous (Florida 2000)
- Voters need to travel (and be in NL).

Voting Machines

- Widely used in NL & IRL
- Main supplier: Nedap
- Internal mechanics is secret
- Evaluation is required, done by TNO
- Evaluation reports are secret

Voting Machines, continued

Advantages

- automatic processing of results: efficient and fast
- vote expression is unambiguous

Disadvantages

- "Processing gap" between expression and recording of the vote.
- Recount only possible on already processed votes
- Voter cannot verify that the vote is registered correctly
- Voters need to travel

US Discussion on paper trails

- The voting machine prints a paper when the voter has finished
- The voter inspects the printout, and if it is correct deposits it in a special box
- The machine provides a preliminary total
- The paper ballots are used for a recount, if requested.

Around 1000 computing professionals have signed a petition urging that all voting machines include such a voter-verifiable audit trail.

Probably it will be demanded by US federal law.
Also in next generation of voting machines in NL?

Voting machines, conclusion

"Consequently, the integrity of elections rests on blind faith in the vendors, their employees, inspection laboratories, and people who may have access—legitimate or illegitimate—to the machine software"

"Democracy should not depend on blind faith"

(From: Dill, Schneier and Simons, *Voting and Technology: Who Gets to Count Your Vote?*, Communications of the ACM, August 2003)

Voting machines, looking back

- The introduction of these voting machines in NL around 1998 was uncontroversial
- Openness (of software) was not an issue at the time.
- Currently controversy in IRL, and questions in NL parliament
- By now we know better about the unreliability and vulnerability of software and networks ....

Next step . . . online voting systems

- **Main advantage**: voters don't need to travel, or be in NL. This may increase participation.
- **Main disadvantage**: security risks.
  - online systems are accessible by hackers
  - centralisation increases vulnerability
  - individual freedom to vote is not guaranteed at home
  - also processing gap between expression and registration of votes.

III. Computer Security Essentials

Computer Security

- Topic: regulating access to assets
- Approach
  - ***Authentication:*** Who are you?
  - ***Autorisation:*** What are you allowed to do?
- Organisation: proper mix of technical, organisational and legal measures
- Technical tool: Cryptography (encryption)
- Weaknesses:
  - Implementation
  - People (both outside and inside!)

Security & Voting issues

- How do you authenticate voters online?
  (There is no national smart card in NL)
- How do you keep voting confidential—at home, in traffic, and after recording?
- Same for integrity.
- How can you keep the system available and prevent "denial of service" attacks?
- How can you make people trust the system?

IV. Planned Voting System in NL

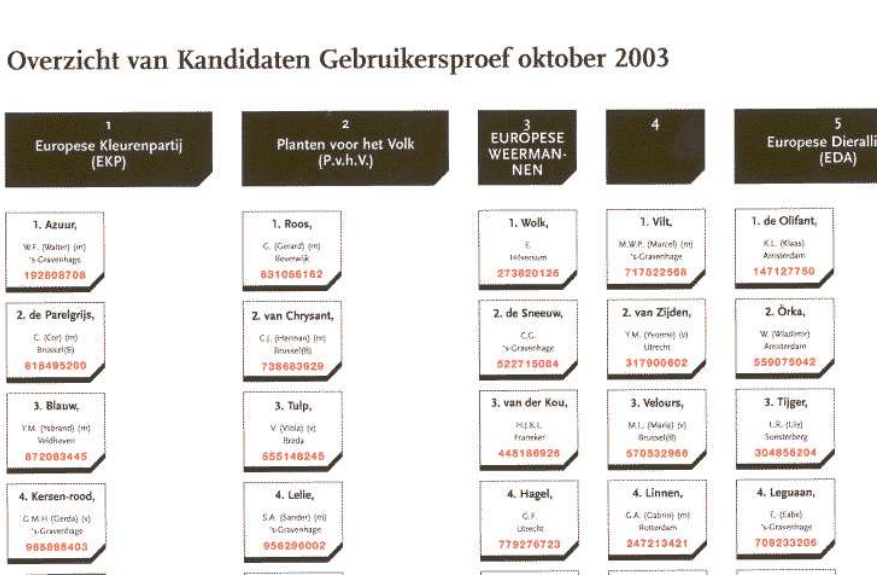
Background

- Open bidding won by LogicaCMG, to set up a voting ***service*** (early 2003)
- Experiments and evaluations, notably by third parties, in second half of 2003
- Limited, one-time, low-tech experiment modeled after voting by (ordinary) mail:
  - Explicit registration with user-defined access code (as PIN, or password)
  - Confidentiality & integrity not guaranteed at home
  - Usually 20-30,000 mail votes, out of about 600,000 expatriats
- Phone as alternative for internet

Codes, codes, codes, . . .

Code	Distribution	Function
voter code (*stemcode*)	after registration	identification when voting
access code (*toegangscode*)	at registration (self-chosen)	authentication when voting
candidate code (*kandidaatcode*)	in ballot (see next slide)	choice
transaction code (*transactiecode*)	after voting	participation check after election

Ballot form, one for each voter


Overzicht van Kandidaten Gebruikersproef oktober 2003

1 Europese Kleurenpartij (EKP)	2 Planten voor het Volk (P.v.h.V.)	3 EUROPESE WEERMAN-NEN	4	5 Europese Dierallí (EDA)
1. Azuur, W.F. (Walter) (m) 's-Gravenhage 192608708	1. Roos, G. (Gerard) (m) Beverwijk 831066162	1. Wolk, E. Hilversum 273820126	1. Vilt, M.W.P. (Marcel) (m) 's-Gravenhage 717022568	1. de Olifant, K.L. (Klaas) Amsterdam 147127750
2. de Parelgrijs, C. (Cor) (m) Brussel(B) 818495290	2. van Chrysant, C.J. (Herman) (m) Brussel(B) 738683929	2. de Sneeuw, C.C. 's-Gravenhage 522715084	2. van Zijden, Y.M. (Yvonne) (v) Utrecht 317900602	2. Orka, W. (Wladimir) Amsterdam 559075042
3. Blauw, Y.M. (Yolbrand) (m) Veldhoven 872083445	3. Tulp, V. (Viola) (v) Breda 555146248	3. van der Kou, H.J.K.L. Franeker 445186926	3. Velours, M.L. (Marie) (v) Brussel(B) 570532966	3. Tijger, L.R. (Lily) Sonsterberg 304856204
4. Kersen-rood, G.M.H. (Gerda) (v) 's-Gravendage 985886403	4. Lelie, S.A. (Sander) (m) 's-Gravenhage 956296002	4. Hagel, G.F. Utrecht 779276723	4. Linnen, G.A. (Gabrie) (m) Rotterdam 247213421	4. Leguaan, E. (Eabe) 's-Gravenhage 709233206

What happens in internetvoting

1. Voter uses webbrowser to contact `www.internetstembureau.nl`, and establishes a secure SSL connection (padlock!)
2. Identification & authentication, resulting in check
3. Vote is cast, after confirmation of choice
4. Vote is recorded, in encrypted form
5. Voter gets transaction code, as confirmation of recording
6. At the end, encrypted database of votes is extracted
7. Decryption by head of voting station, and count.
8. Recount, if needed, on basis of ***same database*** of processed votes.

Some security issues & questions

- Protection of webserver (intrusion, denial of service)
- Protection of communication: voter must check SSL-certificate in padlock
- Influence of system administrators: procedural measures
- Recording of “raw data” from webserver for recount?
  - Blinding is necessary for confidentiality (no IP addresses visible!): “logging tension”
- Personalised ballots give better protection?
  - More confusion likely
  - People may feel being watched

V. Trust and Openness Issues

How to ensure trust in online system?

- Work with reliable parties (builders, evaluators, operators)
- Compartimentalise the whole system, and assign different parts to different parties
- Stimulate public discussion, and hope for endorsement by independent experts & opinion leaders
- Make public how the system works: esp. make it **open source**!

  (First done in Austriala, see `www.elections.act.gov.au`)

Openness & Security

- Within security there is a natural tendency towards secrecy: information helps the attacker
- Modern perspective: openness also gives security, esp. in the long run, because:
  - public inspection gives better error detection
  - backdoors become visible
  - "security by obscurity" does not work: it will be on the internet sooner or later (see Microsoft)
- Openness & transparancy even more important for public tasks
- Dutch Parliament: government should use open standards and open source (*Motie Vendrik, 20/11/02*)—resulting in `ossos.nl`

Code comparison: Lock

Would you have most trust in the locksmith who:

- keeps the working of his locks secret, so that thieves cannot exploit this knowledge?
- publishes the workings of his locks, so that
  - everyone can judge how good/bad they are,
  - one relies on the complexity of the keys for protection?

Open/closed source essentials

- Programs are written as ***source code***, which is reasonably understandable (if .. then .. else).
- They are "compiled" to ***executable code***, which:
  - actually runs on computers (as .exe)
  - is not understandable by humans (0s and 1s)
- ***Closed source distribution*** means
  - the "binary" executable code is distributed
  - very few people know and have checked what code really does (too little or too much)
  - heavy dependence on supplier
  - examples: windows, internet explorer, ...

Example: Diebold voting machines

- Diebold produces closed source voting machines used in US: controversy about political links & security
- Source code put by accident on web
- Analysed by Avi Rubin (`http://avirubin.com/vote/`)
- Results are shocking
  - sloppy programming style
  - elementary security mistakes
  - many, simple, undetectable exploits possible
  - conclusion: public scrutiny essential
- First of several similar investigations. Diebold's standard reaction: we fixed all problems!

Openness in online voting in NL

Own experience: Ministry (BZK) has:

- increasingly strong "nothing to hide" attitude (but confidentiality until minister reports to parliament)
- healthy distance towards supplier
- many evaluations, by several third parties
  - first experiment (august 2003) full of shortcomings
  - second one (october) much better: green light
- rights to software, and has intention to go open source (mode to be determined)

V. Concluding remarks

Conclusions

- Electronic voting can be good use of ICT
- NL is early adopter
- Limited, cautious & low-tech experiment is wise approach
- Scaling to national level requires different set-up (esp. for authentication, and freedom/force/sale)
- Vulnerability of software & networks must be compensated by additional checks (like paper trails)
- Openness is essential, both for security & trust!

Final judgement postponed, until all data are on the table