University of Twente

Verifiability of electronic voting:

between confidence and trust

Wolter Pieters

Radboud University Nijmegen

University of Twente
The Netherlands

University of Twente
The Netherlands

My background

- Masters computer science & philosophy of science, technology and society (Twente)
- 2003-2007 PhD candidate, Security of Systems group (Nijmegen), thesis on e-voting
- 2007-2008 policy officer Ministry of the Interior, e-voting and travel documents
- 2008- postdoc information security (Twente)

University of Twente
The Netherlands

Outline

- The e-voting debate in the Netherlands
- Trust in e-voting
- Verifiability in e-voting
- Verifiability and trust

University of Twente
The Netherlands

The e-voting debate in the Netherlands, 1990

Nedap voting machine

The e-voting debate in the Netherlands, 2007

University of Twente
The Netherlands

The e-voting debate in the Netherlands, 2007

University of Twente
The Netherlands

The e-voting debate in the Netherlands

Questions:

- How did the Dutch e-voting lose its trust?
- Too much trust in the first place?

University of Twente
The Netherlands

The e-voting debate in the Netherlands

My thesis:

- Due to the pressure group Wij Vertrouwen Stemcomputers Niet, e-voting is now seen as really *different* from paper voting
- Therefore, voting is now required to have *trust* rather than *confidence* only: a *decision* must be made by *comparing* the alternatives
- This *by itself* makes paper voting more attractive

Confidence and trust

physical record of their vote and deposit it in a secure ballot box, voter trust in DRE equipment depends on trusting the voting machine hardware and software in combination with the people and procedures designed to safeguard it.

Increasing trust

Several mechanisms have been proposed to provide voters with increased confidence that their vote is cast as in-

on trust in those companies' integrity and expertise.

Voter-verifiable ballots

One way to decrease the trust voters must place in voting machine software is to let voters physically verify that their intent is recorded correctly. Rebecca Mercuri has proposed a method for voter-verifiable ballots. After a voter has finished making selections using a DRE machine, the machine prints out a paper ballot that contains the voter's selections for each choice. The printed ballot is

in "A Brief Illustrated History of Voting" available at www.cs.uiowa.edu/~jones/voting/pictures/.

Recent cryptographic voting schemes, such as David Chaum's,[1] VoteHere (www.votehere.com), and Prêt à Voter[2,3] provide strong security and privacy guarantees, high levels of transparency, and require only a minimum amount of public trust in voting devices or voting officials. In these schemes, *voter verifiability* assures accuracy and preserves ballot secrecy by allowing voters to verify that their votes are accurately counted. However, a full appreciation of such cryptographic voting schemes—on which an entire election's validity would depend—requires a high degree of mathematical sophistication; experts' evaluations and assurances might not be enough to persuade the public to put their trust in such schemes.

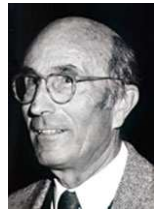
Our ultimate goal is an e-voting system that isn't only completely *trustworthy*—doesn't lose, add, or alter ballots, for example, or violate ballot secrecy[4]—but is also *trusted* by voters to have these properties. As a step toward this goal, we have aimed to develop voting sys-

Wait a minute... do we wish to *minimise* or *maximise* trust?

Confidence and trust

According to Niklas Luhmann, there are two modes of self-assurance relations: *confidence* and *trust*

	confidence	trust
type of reliance	unconscious	conscious
interpretation	no perceived alternatives	comparison of alternatives
action	no decision	decision/choice
what scientists want	minimise	maximise



Explanation of the e-voting debate in NL

- E-voting was never seen as a real *alternative* to paper voting, so that trust was not required
- The pressure group Wij Vertrouwen Stemcomputers Niet made e-voting an alternative, by explicitly drawing the distinction

history/
progress

alternatives

Explanation of the e-voting debate in NL

- Comparing the alternatives required trust instead of confidence only
- Paper voting is less easy to use (confidence), but easier to understand and analyse (trust)
- *The fact that e-voting is now seen as an alternative by itself makes paper voting more attractive*

Verifiability

(Acceptable?) solution: build an *indirect* trust relation for electronic voting:

voter – expert – voting system

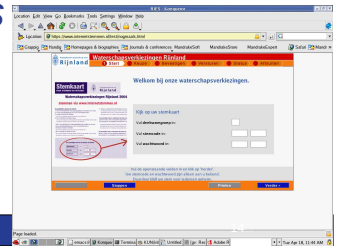
Voter has confidence in expert; expert trusts voting system

Verifiability

Verifiability

- of the *machines / software*
  - only experts involved

- of the *results / calculations*
  - may enable / require participation of the voter



Verifiability

- individual: voter can verify that her vote is included in the results
- universal: independent parties (possibly voters) can verify that the result is calculated correctly based on the included votes

Verifiability

- classical: mathematical proof of vote inclusion / result calculation, without revealing the contents of the individual votes
- constructive: votes are *witnesses* of the inclusion / calculation, may be repeated by independent parties

Verifiability

- Classical individual:

University of Twente
The Netherlands

Verifiability

- Constructive individual:

University of Twente
The Netherlands

Verifiability

- Classical universal:

University of Twente
The Netherlands

Verifiability

- Constructive universal:

Example 1: paper voting

- classical individual verifiability: ballot box guarantees that vote is included, but I can't see which vote is mine
- constructive universal verifiability: recounts are possible based on votes in ballot box

Example 2: RIES

- constructive individual verifiability: voter can verify *for which candidate* her vote has been counted
- constructive universal verifiability: since votes can be linked to candidates, anyone can calculate the results from the received votes

```
Archive:  RT_0.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
       220  08-25-04 09:31   008AB1E98AEDFBA450A1813DDC153553
       220  08-25-04 09:31   08677B73378E1D59153DE30263A3C47C
       220  08-25-04 09:31   06CAC042AF7D6940DD8A51814E68DFF8
       220  08-25-04 09:31   00FEA51461FBF7B406554EEF2E23554D
       220  08-25-04 09:31   05C02BD8E3863DB24D6C332A17B78EFB
       220  08-25-04 09:32   070C60BFFC06B7355425E6FFADBBED30
       220  08-25-04 09:32   034C37BA687E21477D38A110954207B8
---------                     -------
      1540                   7 files

008AB1E98AEDFBA450A1813DDC153553:

vervangend=0
verstrekt=1
vervallen=0
AC9498374305833 4B25452E0F63A9C20=0101020401
B0015BAC8ECF766DB67825592DC10957=0101020402
ACE4213255CA8184D18E0293FF7EE8=0101020403
358AAB0C934757ACCF071A1CD732EDEA=0101020499
```

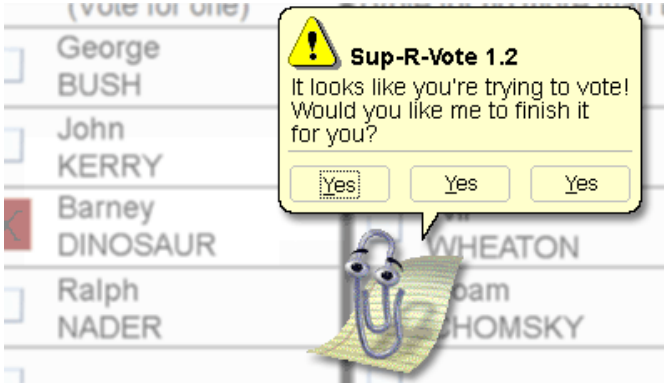

Example 3: most scientific literature

- classical individual verifiability: voter can obtain proof *that* her vote has been included, but not for which candidate
- classical universal verifiability: servers provide mathematical proof that they did not change votes

Verifiability and trust

- what value does mathematical proof provide to voters?
- what about the secret ballot and coercion-resistance?
- least invasive: classical individual verifiability + constructive universal verifiability (same as paper voting)
- no such system yet (even possible?)

We still need to think how to do it!



University of Twente
The Netherlands

More information

- Wolter Pieters. Acceptance of voting technology: between confidence and trust. In: K. Stoelen, W.H. Winsborough, F. Martinelli and F. Massacci (Eds.), *Trust Management: 4th International Conference (iTrust 2006), Proceedings*, LNCS 3986, Springer, 2006, pp. 283-297.
- W. Pieters. What proof do we prefer? Variants of verifiability in voting. In P. Ryan, S. Anderson, T. Storer, I. Duncan, and J. Bryans, editors, *Workshop on e-Voting and e-Government in the UK*, pages 33-39, Edinburgh, February 27-28 2006.

- http://www.cs.utwente.nl/~pietersw
- w.pieters@utwente.nl
- http://www.wijvertrouwenstemcomputersniet.nl