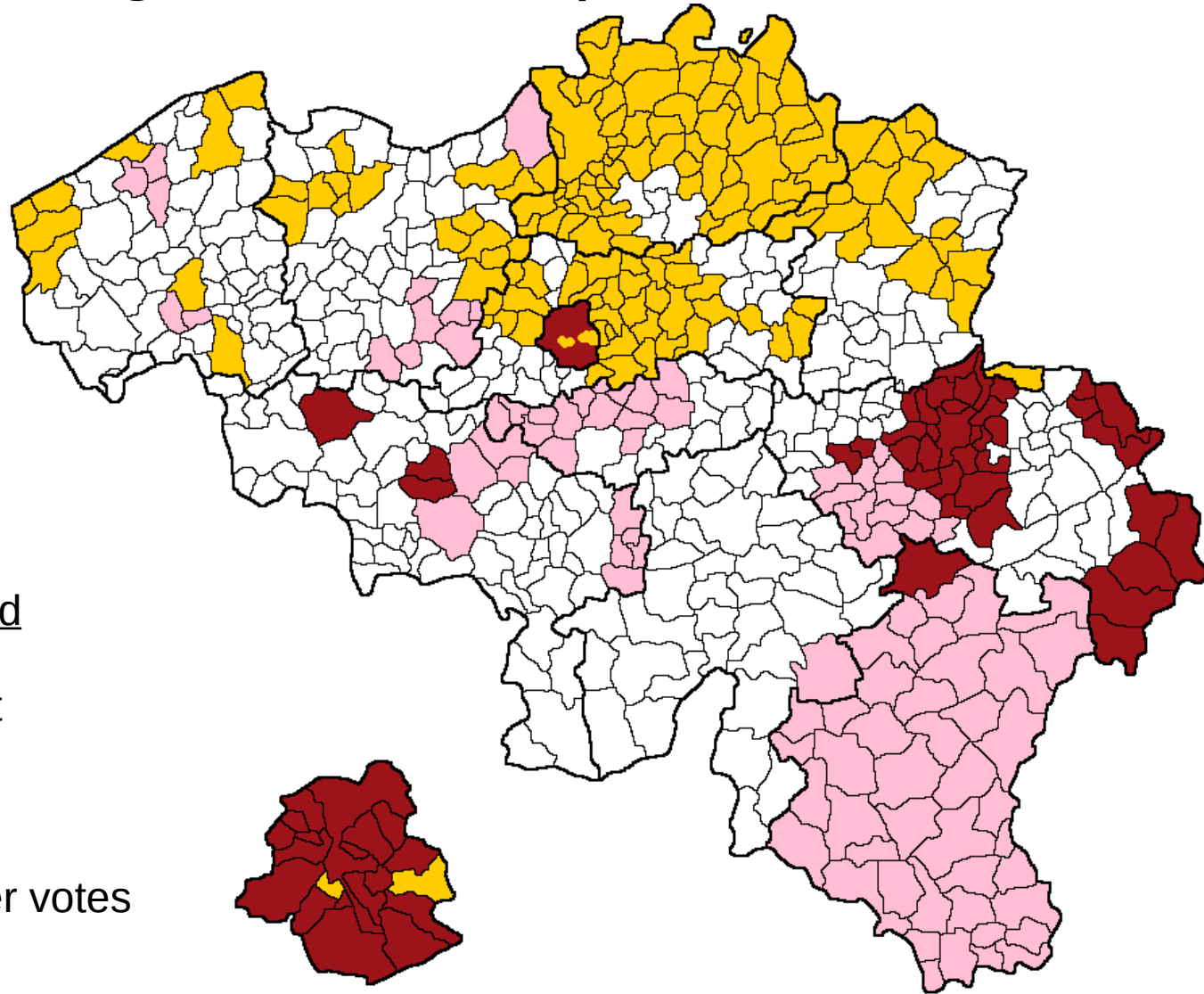# #bug2505

25/05/2014

Belgian federal, regional & European elections

★ eVoting with <u>magnetic card</u>

★ eVoting with paper receipt

★ eSorting of paper votes

☆ Traditional sorting of paper votes

Yes, we're in 2014...

eVoting with magnetic cards in Belgium

Since 1991

Long story...

- DIGIPASS v1, v2 & JITES v1, v2
- providers: Stéria & Stésud
- mutations and cross-overs

2014: JITES

- based on code from 2006
- updated in 2012
- merged with feature from 2010: possibility to deselect votes

25/05/2014

We vote

Evening: counting program (CODI)
flags incoherences in <u>preference votes</u> totals

Big mess, Stésud sent to write quickly
an ad-hoc tool to decrypt votes from floppies...

48h later SPF Intérieur speaks

Incomplete bug description

They say no impact on seats

Can we trust them?

Panel of Experts: bound by secrecy till...
it's too late for legal recourses...

3 days later: source code

Tedious, error-prone, hard to share outcomes
(first conclusions were partially wrong)

Got asked to cross-check

PoC || GTFO

Let's revive that code!

More confident in conclusions

Nicer to show

But...
MS DOS, floppies, optical pen, magnetic cards,...

PoC in 12 hours... under Linux

- Remove hardware libraries, emulate minimum
- Rewrite file IO and other MS DOS parts
- Bring libXbgi, a Xlib-based port of Borland Graphics Interface
- Fix numerous compilation issues (Borland again)
- Recode DOS charset in Latin1
- Run in test mode, skipping floppy crypto
- Create fake election data
- Fix main loop to read back the "card" buffer

DEMO
(sorry cannot get GIF in PDF, see at
http://www.poureva.be/IMG/gif/DemoBugVE.gif)

The bug

- ArrayLists[4]=1 (SP not cleared)
- ArrayLists[3]=1 (Ecolo)
- CardWriter() :
  for(i=...) if(ArrayLists[i] == 1) iList = i + 1 ;

  SP->Ecolo=SP (bogus vote without prefs)

  Ecolo->SP=SP

  More than a preference vote problem!

Resources

git clone git://git.yobi.be/git/EL_2014.git

http://www.poureva.be/spip.php?article853

Panel of Experts report, very nice!

– Bigger mess, final countdown: 5th of June

– Stésud ad-hoc tool didn't detect all faulty votes

– Panel of Expert wrote their own tool...

"the GREP method"