Needs for a Dependability Case for an E-voting (Electronic voting) system

report by Lorenzo Strigini

of work in progress with *Eugenio Alberdi*, Philippe Palanque, Peter Ryan, Kieran Leach, Marco Winckler, and many colleagues in projects RESIST and INDEED at

IRIT @ Université Paul Sabatier, Toulouse, City University London, University of Newcastle

research report at 55th Meeting of the IFIP WG 10.4 on Dependable Computing and Fault Tolerance
Cortina d'Ampezzo, Italy, 28-30 January 2009

Why

Innovative, *really trustworthy* E-voting methods are a hot topic

there is a GAP in the literature:

- many papers demonstrating how a design would work
- but suppose you were advising a state about adoption of a specific implementation.....

You'd want a **Dependability Case**:

- "A documented body of evidence that provides a demonstrable and valid argument that a system is adequately dependable/safe for a given application and environment over its lifetime."

An *E-voting system* is a large, complex, integrated socio-technical system:

- Technological components (hardware, software)
- Human, social factors (diverse people involved in the process with many different roles; adversaries potentially trying to corrupt the system)
- studying a specific system : *Prêt à Voter*

A simplified history of evolution of E-voting ideas

(in the rich world):

1. paper-based, and electromechanical "machine-assisted vote"
   - well-loved but full of holes
2. solution: computers! ("computers don't make mistakes")
   – needs lots of "trusted" software
   – votes disappear into the machine
3. solutions: use software for efficiency and accuracy, but keep independent verification
   – paper trail for recounts
   – or *cryptographically based voter verification*
      * Chaum, Randell & Ryan, Ryan & Schneider, ...
      + one of which is *Prêt à Voter*, our case study

Prêt à Voter in a nutshell

- based on public-key crypto and an intuitive, paper-based user interface
- no need for expensive ad hoc machinery
- encrypted votes and decryption/counting results are visible on a web bulletin board
- each voter receives a receipt
  – allowing him to verify that his vote is being counted
  – but no-one to guess how he voted
- decryption, counting in multiple phases performed by mutually suspicious parties

it's magic!

- will a specific implementation work with real voters, politicians, machines, election officials, adversaries?

What you need for a dependability case

- what are the *claims* made?
  - for a start ... what were the requirements?
- what are sound arguments for believing such claims
  - for a real, flesh-and-blood-and-copper-and-silicon system?
- where would one get the evidence to support these arguments?

- even just asking the questions will help!

- a quick sampler follows

so, what were the requirements?

many different formulations of requirements for E-voting

- top-level, intermediate, system type-specific often mixed

we extracted 4 top-level requirements

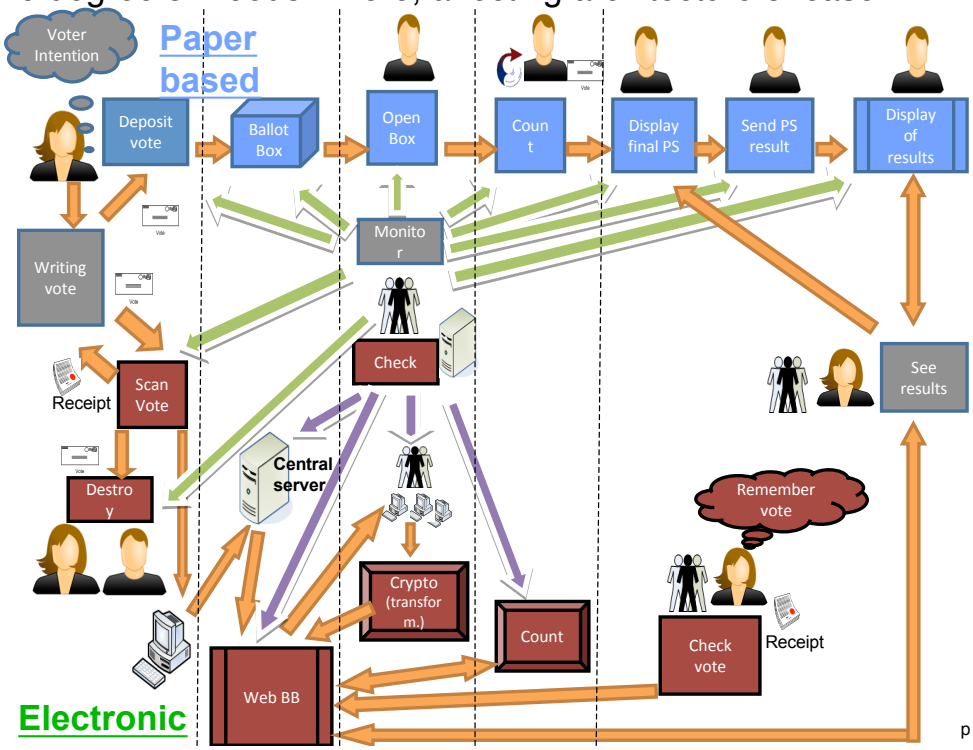
- ACCURACY
- PRIVACY
- SUCCESSFUL TERMINATION
- TRUSTEDNESS

- important first piece of insight: contrasts and needs of trade-offs

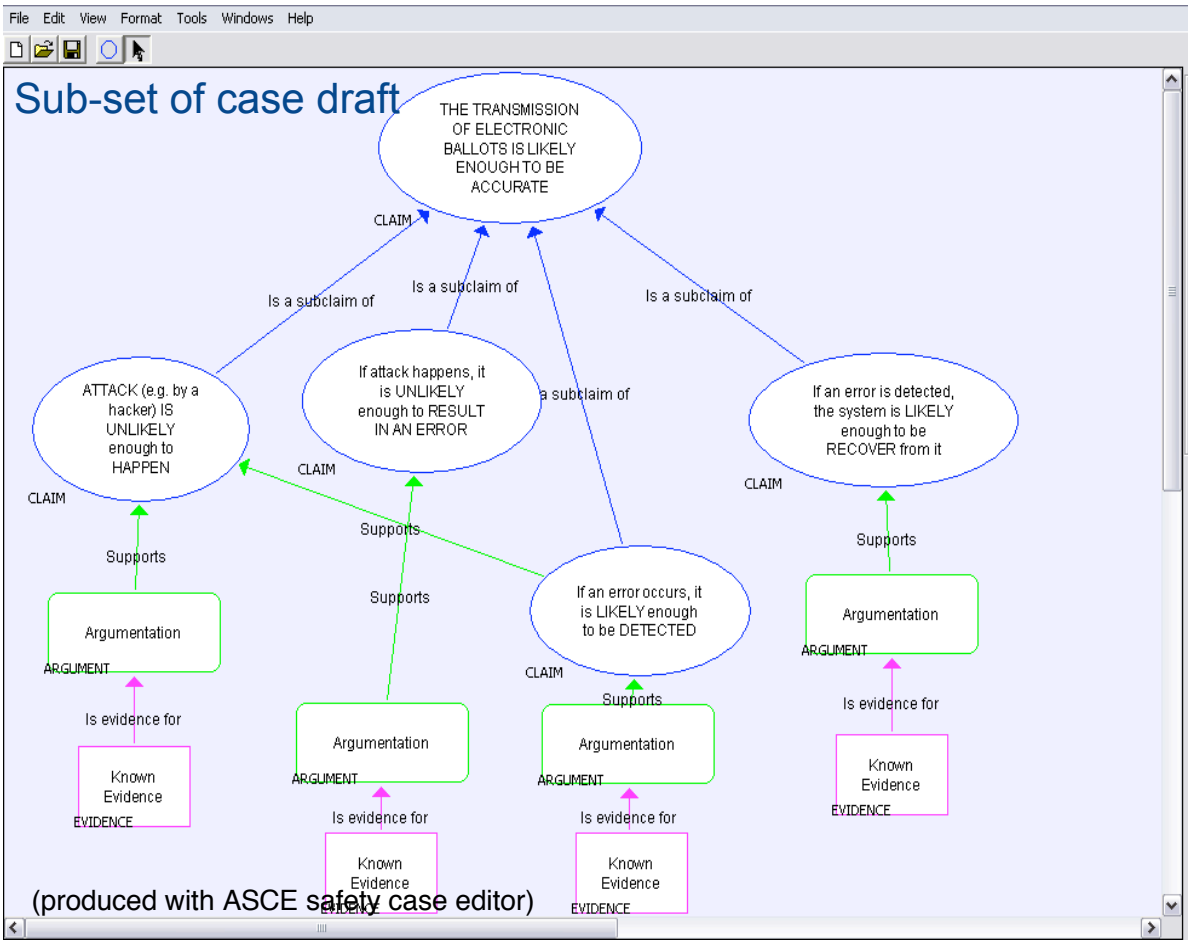
- what *level* for each requirement?
  - "worst-case acceptable probability distribution for counting error"?
    no: "at least as good as" requirements
  - "PaV vs POPS" case
    (Prêt à Voter *vs* Plain Old Paper System)

To decompose the case along architectural lines..

- you need to map PaV architecture on POPS architecture
- some degree of freedom here, affecting architecture of case



p 7



Questions?