# Software Independence and Encouraging Innovation in VVSG 2007

**Presentation for the**
**Technical Guidelines Development Committee (TGDC)**

**Prof. Ronald L. Rivest, MIT**

**December 4, 2006**

# Outline

- Software Independence
- Encouraging Innovation
- Presentation of Resolutions (3)
- Discussion

# Summary of STS Recommendations

- Recommends “Software Independence” as requirement for voting systems in VVSG 2007
  - recommends NIST focus on current SI VVPR systems
- Recommends that VVSG 2007 include a process for considering new SI approaches such as end-to-end, and recommends new, innovative, possibly paperless SI approaches be encouraged.

# Software Independence

# Software-based voting systems

- Software is, on the one hand, wonderful: it enables design of rich, flexible, and powerful systems and of adaptable interfaces for voter.
- On the other hand: *all software is buggy!* Typically 4-5 bugs per 1000 lines of code.
- From a practical point of view, it is impossible to write bug-free code for a large system.

# *Software (in)dependent* voting systems

- A voting system is *software dependent* (SD) if an undetected bug in or modification to its software can cause an *undetectable* change in the election outcome (i.e., not detectable even in post-election audit or recount).
- A voting system is *software independent* (SI) if it is not software dependent.

# Software Independence

- "SI" suggested as a more useful term for VVSG 2007 than VVSG 2005 term "IV", although they are fairly close in meaning.
- Use of "SI" terminology emphasizes the most significant problem: relying on the correctness of software for the correctness of election results.
- SI voting systems are those for which the correctness of an election outcome is not critically dependent on the correctness of its software.
- In practical terms, SI systems have the property that cast vote records and election results can be audited.
- *"Verify the election, not the system."* (Benaloh)

# Software Dependence

- With a SD system, you must assume that system software is correct and unmodified, in order to conclude the correctness of the election results.
- Note: “software” also means firmware, hard-coded logic, etc, all of which are software-based.

# Why Not Software **De**pendence?

- Future voting systems will continue to grow larger and more complex.
- Assuring that complex software is correct is, for all practical purposes, impossible.
- Software is difficult and expensive to test to high degrees of confidence; typically only doable for very small systems.
- Voting system software would need to be stripped down, e.g., no large COTS O/S, and strict design and development methodologies would need to be followed rigorously; this would be very costly yet correctness would undoubtedly still be questioned.

# Requiring SI in VVSG 2007

- *STS concludes that SD approaches should not be permitted in VVSG 2007* and that SI approaches should.
- (Paperless) DRE's are SD, and thus would no longer be permitted. (🡐 *Significant change*!)
- VVPR systems are SI, and so would be allowed.
- This effectively means, for now, writing requirements primarily for VVPR systems
- *But*: STS recommends that new, innovative, potentially paperless SI approaches be encouraged (e.g. end-to-end systems).

# Future SI Approaches

- There are many possible approaches to SI.
- E2E (End-to-end) systems
  - Voters may audit that their ballots were counted as cast (stronger security than provided by typical VVPR system)
  - Uses paper receipts, not paper records
  - May use cryptography
  - E2E may support greater usability and accessibility
- Software IV? - STS debates whether versions of software IV should be considered in the SI class.
  - Probably not--some reliance on s/w seems necessary
  - Still, it holds promise
  - Many variants exist; many practical issues to be resolved
  - Recommend that NIST remain focused on paper IV (VVPR)

# Ramifications of Requiring SI

- Does requiring SI in VVSG 2007 mean existing equipment will be decertified?
- Answer: ***NO*.** VVSG 2007 is written for *new* equipment, not for current systems.
  (As with VVSG 2005, current systems can in effect be ‘grandfathered’.)
- Note: Requiring SI should not be interpreted to mean that existing DRE systems are in fact insecure, just that there are no good ways to evaluate their security.

# What About Existing DREs?

- Does requiring SI in VVSG 2007 mean existing DRE's need to be replaced immediately?
- Answer: ***NO*****.** For at least two reasons:
  - Cost: Some states have just invested in their DRE's, and it would be expensive to replace them. A state may need to get a reasonable amount of use out of these machines before replacing them.
  - Security: As noted, the STS is not arguing that these machines are *insecure,* just that it is very difficult (or impossible) to tell if they are secure or not. There is no specific reason to believe that these machines are reporting incorrect election results. However, the extreme difficulty of assessing the security of these machines makes it inadvisable to consider such software-dependent machines within VVSG 2007.

# What if We Don’t Require SI?

- It appears impossible to write requirements to secure SD approaches---no reasonable amount of testing will guarantee bug-free code.
- If we attempt to write requirements for SD, we’ll either have to “trust the vendor” to write correct code (!), or else incur unacceptably large development and testing costs.
- If we don’t require SI, Congress may do it for us, by mandating voter-verified paper trails.
- We may be able to do it better: “software independence” is better overall approach than merely mandating voter-verified paper records, in the long run.

# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT

# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Non-VVPR
  - Lever
  - DRE

# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Non-VVPR
  - ~~Lever~~
  - DRE

# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Other/New
  - End-to-End
  - Software IV
- Non-VVPR
  - ~~Lever~~
  - DRE

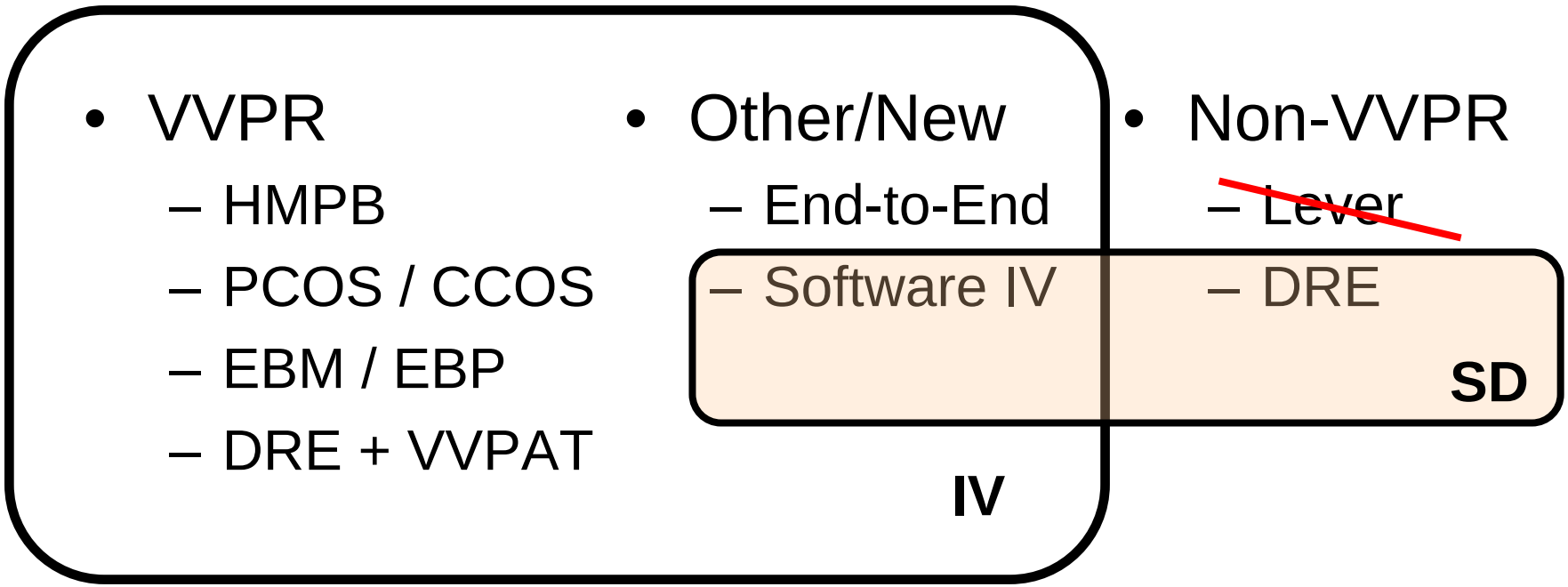
# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Other/New
  - End-to-End
  - Software IV

**IV**

- Non-VVPR
  - ~~Lever~~
  - DRE

# Voting System classes



# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Other/New
  - End-to-End

**IV**

- Non-VVPR
  - ~~Lever~~

- Software IV
- DRE

**SD**

# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Other/New
  - End-to-End

**SI**

- Non-VVPR
  - ~~Lever~~

- Software IV
- DRE

**SD**

# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Other/New
  - End-to-End

**SI**

- Non-VVPR
  - ~~Lever~~

~~– Software IV~~ ~~– DRE~~

~~**SD**~~

# Encouraging Innovation

# Encouraging Innovation

- We want the voting industry, others, to pursue new and innovative SI systems.
- These approaches could promise greater usability, accessibility, and greater confidence and accuracy in future elections.
- For example, software IV might eventually achieve the security of VVPR but without paper.
- How do we encourage such innovation?

# The ‘Innovation Class’

- Goal is to ‘open the door’ in VVSG 2007 to promising new SI approaches.
- By explicitly including a way such new approaches can be evaluated within VVSG 2007, we hope to encourage developers.
- Specifically, we recommend including an ‘Innovation Class’ for new approaches.

# Voting System classes

- VVPR
  - HMPB
  - PCOS / CCOS
  - EBM / EBP
  - DRE + VVPAT
- Other/New
  - End-to-End

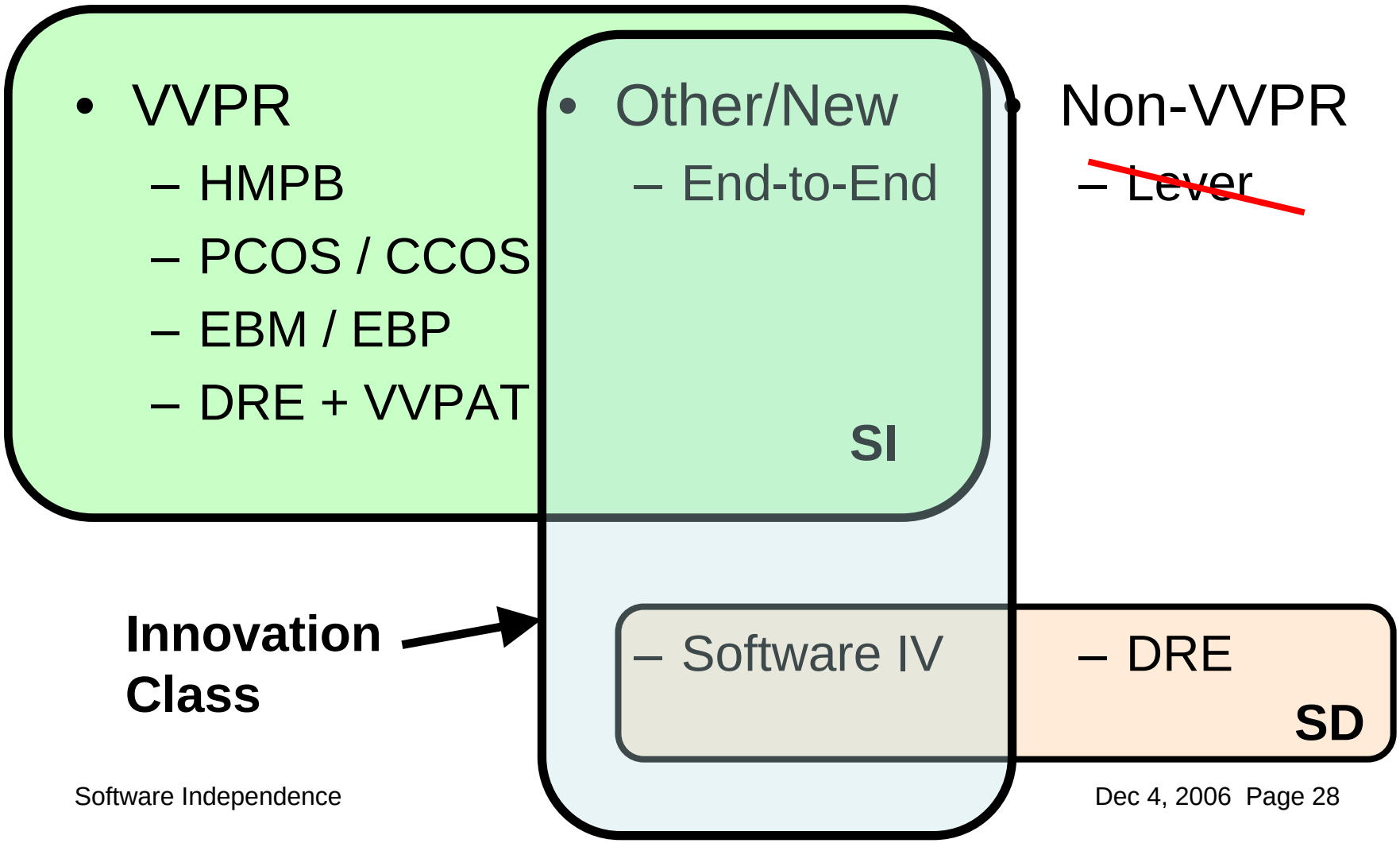
**SI**

- Non-VVPR
  - ~~Lever~~

- Software IV
- DRE

**SD**

# Voting System classes



# How Would This Work?

- STS could develop high-level, guiding requirements and principles for new approaches. (It may be possible to give more detailed requirements for some end-to-end approaches.)
- A developer could submit a system to a VSTL, along with documented proof that the system meets these SI requirements.
- The VSTL could convene an expert review panel to inspect the approach and make recommendations.
- Other expanded testing would be likely, i.e., expanded open-ended vulnerability testing.

# Fostering New Approaches

- New approaches could be risky to invest in, requiring experimentation, trials.
- (I note that U.K. Section on Electoral Modernization is holding pilots using innovative voting methods next May.)
- Some fostering of these approaches could encourage researchers, vendors to pursue them.
- Otherwise, moving to newer, potentially paperless approaches is less likely to occur.

# Funding HAVA Research

- HAVA, PART 3--GRANTS FOR RESEARCH ON VOTING TECHNOLOGY IMPROVEMENTS
- EAC is to make "*grants to assist entities in carrying out research and development to improve the quality, reliability, accuracy, accessibility, affordability, and security of voting equipment, election systems, and voting technology*"
- The TGDC should recommend funding this.

# STS resolution discussion

- Require SI in VVSG2007.
- Recommend that VVSG 2007 include an “Innovation Class” under which new voting system approaches can be evaluated and certified.
- Recommend that HAVA Part 3 be funded to enable the EAC to better encourage the development of improved voting systems.

# Discussion