

Ron Rivest

TGDC Update

[I speak for myself, not for TGDC or EAC or anyone else]

Recall:

TGDC was created by HAVA 2002 and first met in July 2004

- Advisory to EAC
- Chartered with creating voting system guidelines (standards) for federal certification

Progress:

Initial VVSG delivered to EAC May 9, 2005

90-day comment period, 6,599 comments received

New VVSG adopted Dec 13, 2005

Really only update to previous standard

Major changes: accessibility requirements; security—national software reference library, wireless, VVPAT; usability—testing by vendors

Available on EAC website

Annual report for EAC now out, www.eac.gov; also vote.nist.gov

TGDC working on improvements and extensions

VVSGII?? Or modules??

Topics to be addressed:

- Early part of 2006
 - Crypto
 - Access control and system availability
 - Physical security
 - Communications security
 - IDV overview
 - Startup/shutdown requirements
 - Hardware security
- Later in 2006, early 2007
 - System development
 - System maintenance
 - Threat analysis
 - Technical data package (especially security)
- Goal
 - Complete new version by July 2007 (?)
 - Nearer terms (?): OEVT (open ended vulnerability testing)
 - Classic 'penetration testing' operation
 - No-holds barred examination of system
 - Given complete access to source code, system, tools...
 - Model (perhaps) RABA testing of Diebold in Maryland
- Lots of questions
 - Documentation

- Who is examining system (team...)
- What level of effort (man-months? \$\$--needs to be
- Who pays? (vendor?)
- What sort of reports is generated?
- Who gets to see report? (submitted version?)
- How is pass/fail decision made?
- Evaluation of COTS software, ASICS, etc
- Auditing (especially VVPAT systems)
 - System produces multiple records of ballot
 - Electronic—may be used for tally
 - Paper (verified by voter)
 - Paper (barcode on paper??)
 - VVPAT meaningless if electronic \leftrightarrow paper correspondence not checked, at least on sampling basis...
 - How to do this audit?
 - Pick some machines (or precincts) at random, and compare record sets...
 - How many?
 - Math not well represented in law...
 - “1%” not based on analyses...
 - “right math”
 - Collection of apples to check (~precincts)
 - Can test apply to see if bad or good
 - Want good chance ($\geq 95\%$) of detecting fraud (% of bad apples) of 1% or more
 - Right rule: test enough apples so that at target fraud rate (1%) you’ll see three bad apples on average (e.g. 300 apples). Then you’ll find at least one bad apple at 1% fraud rate with probability 95%
For 0.2% fraud 1500 apples needed...
 - Compare electronic and paper records
 - Have people look at human-readable records and computer to electronic versions
 - If human-readable not machine-readable, that’s maybe the best you can do?
 - Bar codes on paper-encoded same as human-readable?
Then 3-way: electronic \leftrightarrow barcode \leftrightarrow human readable
 - Electronic \leftrightarrow barcode maybe automatable (?) -scanning ballots of paper??
 - But barcode \leftrightarrow human readable??
John Kelsey: generate pixel map from barcode, and compare??

Need good designs for VVPAT such that such audits can be done in a way that is easily performed

Not possible: electronic ballot printer, OCR font (ref. my scanning experiments), bring in second manufacturer scanner for audit (portable)

