NJ Voting-Machine Lawsuit

Stephen R. Beard

Team member 2

Team member 3

CAL POLY

Summary

- October 2004 – NJ used over use of direct-recording electronic (DRE) voting machines
- February 5, 2008 – 37 machines in 8 different counties reported more Rep/Dem votes than registered Rep/Dem (!)

  Only explained by a bug of some sort

  “Until this point the State had maintained that these voting machines are 100% accurate.”
- Team of 9 computer scientists allowed to inspect machines in an air-gapped environment for 30 days
- Team found

  standard insecurities (firmware replacement, storage tampering);

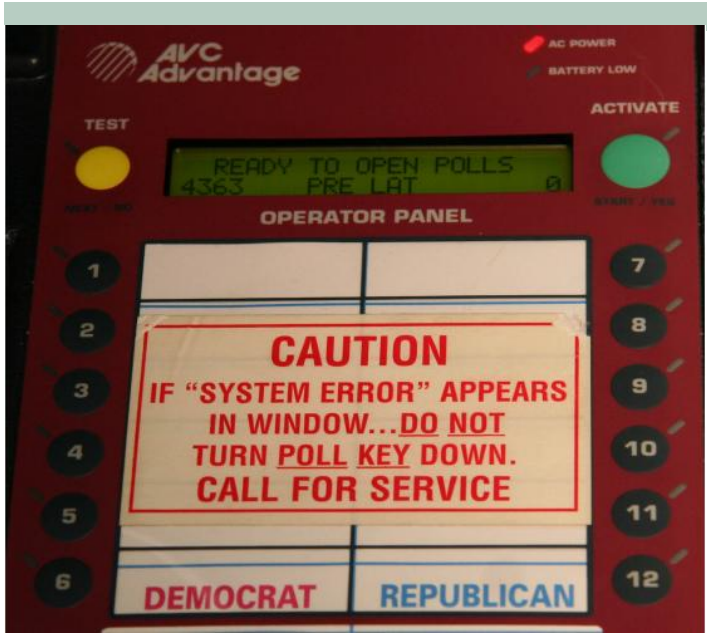
  UI design flaws;

  hardware fault that caused vote disagreement;

  buggy software
- Ultimate (high-level) Finding/Recommendation: ???

Voter Disenfranchising Bug

- Operator supposed to press 6/12 -> Activate
- Any other sequence (6/12 - > another number -> activate) makes the system behave as though it works, but does not properly count votes



Results Cartridges

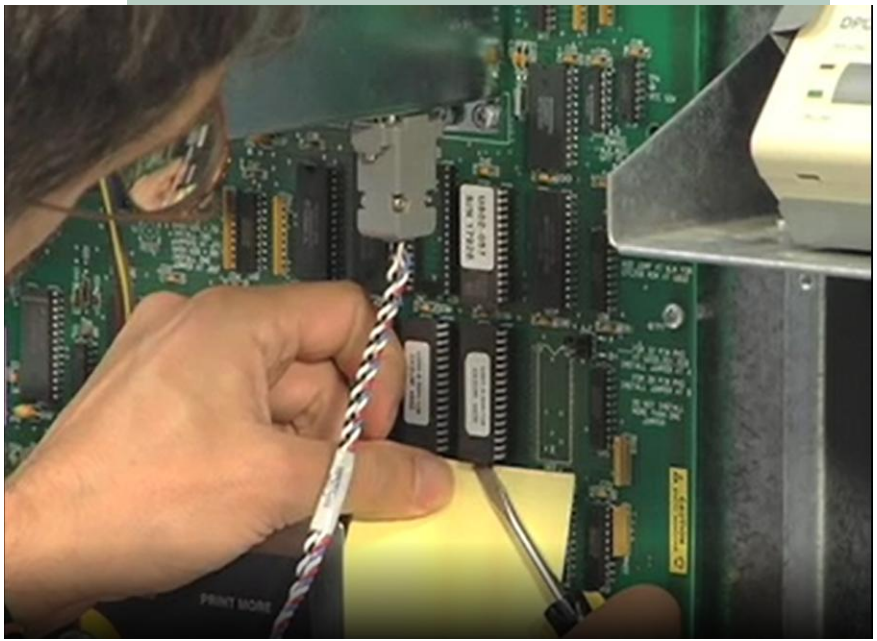
- Votes stored in results cartridges
- Cartridge has no protection, all totals are easily manipulated

Top left: Cartridge reader/writer prototyped by Hovav Shacham's research group [7]. Bottom left: Our nonfunctional mockup of installation in cigarette pack. Right: "Gumstix" computer that could be programmed to alter votes in cartridge.

Firmware Replacement

- Experts showed that it was very easy to replace the voting machine firmware

1. Pick the lock
    1. Appel went from never picking a lock to picking the machines lock in 15 seconds after two days of practice
2. Replace the chip
3. 7 minutes total
4. Physical seals -> easily bypassed
    1. One can remove and replace such seals using very simple tools and techniques, such as “poke with a jeweler’s screwdriver.



Time to ~~Vote~~ PacMan