Voting Insecurity

Barbara Simons

IBM Research (retired)
Board Chair, Verified Voting

Computer Technology Security Issues for this Election

- Electronic voting machines
- Voter registration databases
- Internet voting (David Jefferson)

Computers ain't Perfect

- All large programs have software bugs
  - Voting software is very large
    - Laws differ between and within states
    - Machines have to work everywhere
  - Apple, Microsoft, etc. send out periodic bug fixes
    - Even they can't prevent software bugs
    - Sometimes fixes are for security vulnerabilities
- Software vulnerable to malfunction
  - Voting machines have added, dropped, miscounted votes
- Software may be infected with hidden malware
  - Could impact election results

Electronic Voting Machines

How did we get to where we are today?

- Florida 2000 - paperless touch screen machines as solution to hanging chads
  - 2002 Help America Vote Act (HAVA)
    - Almost $4B allocated to purchase new voting systems
      - Election officials pressured to update equipment
    - No standards, inadequate testing, secret software
    - No accountability of vendors for flaws in software/hardware
- Machines now failing in large numbers
  - Some old software no longer maintained by vendor
    - Way past use-by dates
  - Major cause of long lines in 2012 – likely to repeat in 2016

How is America Voting?

- Computers used almost everywhere
- Polling place: 2 types of systems
  - Direct Recording Electronic (DRE)
    - Touch screen – may or may not have paper
      - If paper, continuous roll thermal printed – like gas station
  - Paper ballots – you fill in (e.g. SATs)
    - Scanner tabulates
- Remote voting (risks of coercion + vote buying)
  - Mail-in ballots – scanner tabulates paper ballot
  - Internet voting (email or web based) – insecure

Diebold: a poster child

- Feb. 2003 Diebold software discovered on open website
  - Software patches written at last minute for system used in Georgia in 2002 midterm – election upsets
    - No independent oversight
- **“...Committed to helping Ohio deliver its electoral votes to the President next year.”**
  - Diebold CEO Walden O'Dell in letter to Central Ohio Republicans, Aug. 14, 2003
- Multiple studies found major security problems

Diebold

- Princeton group: how to planted a virus on paperless Diebold DRE (Sept 2006)
  - Spread by removable memory card
    - Used for upgrades and end of election vote tally
  - Virus could rig an election, corrupt results, or disenfranchise voters by slowing machines
  - Impossible to detect or protect against, because no paper for audit or recount
  - Machines used by >10% of voters in 2006
  - https://www.youtube.com/watch?v=OJOyz7_sk8I

Diebold no longer makes voting machine

- But Diebold paperless DREs still in use
  - All of Georgia, portions of other states
- Other vendors equally bad – Diebold misfortune
  - California Top-to-Bottom Review (D. Bowen; 2007)
    - “We found significant, deep rooted security weaknesses in all three vendors' software...It should now be clear that the red teams were successful not because they somehow “cheated,” but rather because the built-in security mechanisms they were up against simply don't work properly...There was a pervasive lack of good security engineering across all three systems...”
      - Matt Blaze

Paperless vs Paper

- Paperless: Carteret Co, N. Carolina
  - Almost 4500 votes lost in early voting
    - 2287 vote separation in Agricultural Commissioner race
  - Multiple attempts to rehold election
  - Decided by affidavit
  - Unilect Patriot: Still used in Virginia
- Paper: Pottawattamie County, Iowa: Republican Primary
  - Suspicious machine results
  - Manual count changed winners
    - Ballot rotation

“Worst voting machine ever”

- WinVotes crashing in Virginia 2014 midterm
  - Downloading music onto iphones?
- Wireless connection
  - Unchangeable encryption key “abcde”
  - Could download database, change votes, and upload
- Windows CE 3.0; no security updates since 2007
  - Password “admin”
- Decertified by VA
  - Had been used by 568 precincts since early 2000s

President's Commission on Election Administration (bipartisan)

- Created in response to 2012 long lines
- “... the impending crisis in voting technology”
- “[The] machines are now reaching the end of their natural life cycle, and no comparable federal funds are in the pipeline to replace them.”
- “Recommendation: Audits of voting equipment must be conducted after each election ... and data concerning machine performance must be publicly disclosed.”
  - Need paper to conduct audit – should be manual
  - Recommended “risk-limiting” audits

Post-election ballot audits

- 1965 California law requires manual count of 1% of all precincts, randomly selected
  - Way ahead of its time
  - Didn't say anything about escalating the count if problems uncovered
- Evidence based elections: verify that computer-declared winners actually won
  - Only way to check is paper ballot viewed by voter

Risk-limiting Ballot Audits

- Uses statistics to count the “right number” of ballots (Stark)
  - Depends on closeness of race
  - Select probability of correctness, e.g. 95%
    - Number examined: probability + closeness of results
    - If uncertainty, then audit extended
    - Ideally check at individual ballot level, but other options
  - May result in total manual recount
- Provide proof for losers and losers' supporters

Commission's Recommendations Widely Ignored

- The following 5 states are entirely paperless: DE, GA, LA, NJ, SC
  - Georgia may be in play
- The following 10 states are partially paperless: AR, IN, KS, KY, MS, PA, TN, TX, VA; FL for accessible voting
  - Pennsylvania, Virginia swing states
- No meaningful recount possible in 15 states!
- Most states still do not conduct adequate post-election ballot audits, even if they have paper

What can be done in the short run?

- Provide emergency paper ballots for all DREs, whether or not they have paper
  - Poll workers should be instructed to use when lines get long
  - Voters should be reassured that ballots will be counted
- If there is paper, conduct post-election ballot audits to make sure that either computer-declared results are correct or the correct results are obtained via manual tally

What should be done in the long run?

- Replace all DREs with paper ballots
  - Most systems use scanners to record and count ballots
    - Scanners have computers
- Pass laws that reflect the use of computers in our elections
  - Computers can have software bugs or malware
  - Must mandate risk-limiting post-election ballot audits for all elections
    - Should not be responsibility of candidate

GOAL:

Evidence based elections

where it's possible to convince
losers and their supporters
that they have truly lost

NEED:

Voting systems
that can be
audited and recounted

+

Laws that mandate
risk-limiting post-election ballot audits

Voter Registration Databases

Russian hacks?

- Director of National Intelligence and Dept of Homeland Security joint election security stmt:
  - "These thefts [email hacks of US political organizations] and disclosures are intended to interfere with the US election process."
  - "Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government."
    - Oct 7, 2016

Background

- Florida 2000 again
  - Democrats: voters wrongly removed from voting rolls
  - Republicans: non-voters (undocumented, former felons) illegally voted
- Solution: statewide voter registration databases by 2006
- Again no testing, tracking, vendor accountability
- No federal standards, including security

Washington State

- SoS candidate Tina Podlodowski uncovered back door into state voter reg database
  - Vulnerability fixed after disclosed
    - Discovered without doing a full fledged security audit
  - If allowed hacker to modify database, could change voters' addresses or pad voting rolls
    - Washington vote by mail state
- We don't know how many other voter reg databases may have undetected vulnerabilities

AZ and IL databases hacked

- FBI: foreign hackers, possibly Russian state-sponsored aimed at disrupting election
- Probes have targetted election systems in over 20 states
- DHS has offered to help states detect vulnerabilities in their systems
  - 20+ states have accepted offer
  - What about the others???

Why should we worry?

- Voter reg databases contain party affiliation
  - An attacker could selectively disenfranchise voters by deleting names or changing address
  - If done on a moderately large scale, will result in chaos at the polls
  - Voters could be given provisional ballots, but how can voter's legitimacy be verified if no version of correct database available?

What can be done in the short run?

- Election officials must backup voter reg databases frequently and not write over older versions
- Encourage voters to check that they are registered
- Provide paper copy of local voter reg database to each polling place
- Provide sufficient number of provisional ballots as back-up

What Should be done in the long run?

- Map the network to determine if any component can access Internet
- Physically disconnect everything from the Internet
- Employees who can update database should have access only to fields that are part of their jobs
- Close to an election do not allow:
  - Mass deletions or insertions in database
  - Upgrades or modifications of software

Voting is a national security issue

- Should be declared part of critical infrastructure
- “Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.”
    - President Obama, The State of the Union, 2/12/13

https://www.verifiedvoting.org/