Illustrated History of Voting

- Privacy, Reliability, Anonymity, ...
  - Who gets to vote, whose votes are counted?

History of Voting

- http://americanhistory.si.edu/vote/votingmachine.html

Voting, Technology, Internet

- “If elections are defective, the entire democratic system is at risk ... Americans are losing confidence in the fairness of elections, and while we do not face a crisis today, we need to address the problems of our electoral system.”
  - Commission on Federal Election Reform
- From 1876 (Rutheford B. Hayes) to 2000 (George Bush), pushes for “voting machine reform”
  - HAVA, 2002, results?
  - Toward or away from internet voting?

HAVA and Technology

- Section 303(a) of HAVA, 42 U.S.C. § 15483(a), requires each State with voter registration requirements for elections for federal office to implement, through the chief State elections official, a single, uniform, official, centralized, interactive computerized statewide voter registration list. HAVA requires the list to be defined, maintained and administered at the State level, to contain the name and registration information of every legally registered voter in the State, and to assign a unique identifier to each legally registered voter in the State.
Who votes, why is this important?

- 18-24 compared to 45-54:
  - 46% v 69% and 28 million v 41 million
- BA degree, high school, no high school
  - 82%, 57%, 39% and 36 million, 68, and 33

- Internet voting and demographics
  - Digital divide?
  - Dial up compared to ...

Attacking the machines

- How hard is it to hack a paper ballot?
  - What would need to happen?
- How hard is it to attack a DRE machine?
  - What could happen, repercussions?
- How hard is it to attack an Internet vote?
  - How do we guard against this?

Analyzing “difficulty”

- How hard is it to find the phone number of John Smith using a phone book?
  - What about whose number is 914.962.4204?
- How data is organized affects “difficulty”
  - Given a reverse-number phone book...
  - Given Google ...
- Everyone in the room get in line, ordered by age
  - Time, then repeat with twice as many people

Complexity and Computer Science

- Time doubles when number of people double
  - Linear or $O(n)$
- Time increases by factor of four when # doubles
  - Quadratic or $O(n^2)$
- Time doesn’t change when number doubles
  - Constant time or $O(1)$
- Why does this matter?
Attacks (see Wallach paper)

- **Absentee/vote-by-mail**
  - To steal N votes must do O(N) work, bribe or coerce each voter. What about using postal workers? O(N/P)
  - Centralized DoS attack, potentially O(1), throw out all envelopes, all from some zip-code, etc.

- **DRE attack**
  - Anonymity using O(P) or O(1) since order of votes is kept in machine (maybe)
  - Some precincts log order of visits, others would need to do work, but just the Poll workers

Other technologies

- **VVPAT: Voter-verified paper audit trail**
  - Add on to DRE or other systems
  - DoS goes from O(1) to O(P), why?

- **Optical Scan systems (OPS) and Internet at home voting**
  - Which are susceptible and why?
  - What are dangers of Internet voting?

Dissecting IPv4 addresses

- **64.233.167.99**
  - Why is this called a dotted quad?
  - 32 bits/IP address, how many per quad?
  - Total number of values/quad?

- **01000000.11101001.10100111.01100011**
  - What does 64.233.167/24 mean?
  - How many bits do we “use” in routing
  - Related to ICANN/IANA “chunk” sizes, how?

What about IPv6?

- **2001:0db8:85a3:0000:0000:8a2e:0370:7334**
  - There are 8 four-value, hexadecimal parts
  - Each one is 16 bits, so 16x8 = 128 bits/address
  - We don’t need to understand the parts to use IPv6, but we can!
  - 127.0.0.1 becomes ::1/128

- **Duke addresses share a common prefix**
  - Last part “really” identifies you?