Electronic Voting

Matt Bishop
UC Davis

This Is Not About …

- Voting algorithms
  - Take ECS 251 or a distributed algorithms class
- Internet voting
  - We'll point out a few relevancies
- Different voting schemes
- Who will win the next election?

This Is About …

- How electronic voting machines work
- How they fit into the scheme of an election
- How they *should* fit into the scheme of an election
- What can go wrong

Key Question

- Does the use of e-voting machines introduce any *new* vulnerabilities in elections?
  - Paper ballot elections can be hacked

What to Take Away

- E-voting machines *can* be used effectively and accurately
- E-voting machine results *must* be independently auditable
- E-voting machines *must* allow as thorough observation as the use of paper ballots

Outline

- Background
- Non-electronic elections
- Requirements for e-voting systems
- Key questions about e-voting systems
- How to hack an election: the Maryland red teaming
- Conclusions

Terms

- Next election in Davis
  - 2 propositions
  - 8 candidates for 3 City Council offices
- Race: smallest unit upon which a voter votes
  - 3 races in the above election
- Ballot: collection of votes cast in an election
  - 1 ballot containing votes for 3 races above

Over- and Under-votes

- Overvote: voting too many times
  - Vote for 4 candidates for City Council
  - No votes in that race counted
- Undervote: not voting in a race
  - Don't vote YES or NO for Proposition 55
  - Cast votes are counted; votes not cast are not

Background

- Hopkins report
- Diebold's response
- SAIC report
- Problems

Hopkins Report

- *Excellent review of source code*
  - Found lots of software problems
  - Mitigations from procedural mechanisms not discussed or mentioned
  - Threat model assumed malevolent insiders
- Diebold's response made things worse

Diebold's Response

- Hopkins group did not test software under realistic conditions, and used an old version
- Hard-coded password issue "resolved in subsequent versions of the software" (July 30, 2003, p. 11)
- System developed using standard software engineering techniques
- System passed rigorous certification checks
- Not possible to perform attacks suggested by Hopkins team

SAIC Report

- 169 baseline management recommendations made
- 110 operational baseline security requirements
- 47 technical baseline security requirements
  - No source code review performed
  - Deemed met based on the (presumed) integrity of Diebold software and Microsoft Windows CE, 2000
- Also responded to Hopkins report (poorly)
  - *Example*: not feasible to vote multiple times as booth is open (so observable) and ejecting smart card makes a loud sound, so poll workers would notice two cards ejected in sequence when there was only one voter

Non-Electronic Elections

- Go to polling place and give name, address
- Get ballot, enter booth
- Use mechanical punch to punch out perforated holes to indicate vote
- Take ballot cards, put into concealing envelope
- Leave booth, drop envelope into ballot box

End of Day

- Election officials remove ballots from envelopes
- Ballots run through optical scanner to count votes
- Under California law, 1% of ballots from precincts counted by hand, compared to results from optical scanner

Properties

- Voter must be able to vote
- Votes are secret
- Votes are anonymous
- Voter can verify votes at any point before dropping ballot into ballot box

Properties (2)

- Voter can get new ballot any time before placing ballot in ballot box
- Voter votes limited number of times per race, and once per ballot
- Vote tally is accurate and auditable

Role of E-Voting System

- Replace manual punch and paper ballots
  - Easier to configure (164 different ballots in Yolo County for March election!)
  - Can handle multiple languages easily
- Replace hand tallying of votes
  - More on this later …

Requirements

- Must be available
- Must provide simple to use, easy to understand, hard to misuse interface for voter
- Must not be able to associate votes with a particular voter

Requirements (2)

- Must allow voter to discard votes up to the time the voter officially casts ballot
- Must prevent voter from casting more than limited number of votes per race, or once per ballot
- Voter must be able to verify vote up to time vote is cast

Requirements (3)

- Must tally votes accurately
- Must provide an *out-of-bands* mechanism for verifying vote tally

Other Models

- Neumann (1993)
- Saltman (1988)
  - These provide more system-oriented requirements, but those map into the requirements listed above

Points to Ponder

- What OS does the e-voting system use, if any?
- How long does the e-voting system stay up?
- What is the procedure for getting e-voting machine ready to use?

Points to Ponder (2)

- How have you tested the user interface?
- How do you handle write-in votes?

Points to Ponder (3)

- How does the system associate votes with voters?
- Does your authentication/ authorization mechanism associate external voter identities with that information?

Points to Ponder (4)

- What is point at which e-ballot is cast, and voter cannot redo any part of the ballot?
- How do voters change their votes?

Points to Ponder (5)

- How do you check enforcement of limits on voting in a race?
- What support must be provided to ensure that no-one can cast multiple ballots?
- What assumptions does the e-voting system make about procedures and support?

Points to Ponder (6)

- How can the voter verify that the e-voting system accurately recorded votes cast?
- Does this verification require the intervention of a third party?

Points to Ponder (7)

- What requirements is system designed to meet?
- How do you know it meets them?
- How do you handle updating software, hardware on fielded systems?
- What do maintenance people do when they work with e-voting systems?
- How can you verify systems meets requirements after maintenance, upgrade?

Points to Ponder (8)

- What audit mechanism, external vote tally, does the system supply and how do you know it is correct?
- How could an auditor use this mechanism to validate results of an election?

Key Ideas

- Separation of Privilege
  - Observers can check everything in paper election
    - Not with e-voting systems to the same degree
- Auditability
  - Maybe with e-voting systems …

VVAT

- How can voter know whether her votes tallied accurately?
  - Some sort of paper trail
  - Required by law in California for all new e-voting machines after March 2004, and cannot use e-voting machines without them after 2006
  - County Recorders did not like this
    - A few loved it, though

Attacking a Voting System

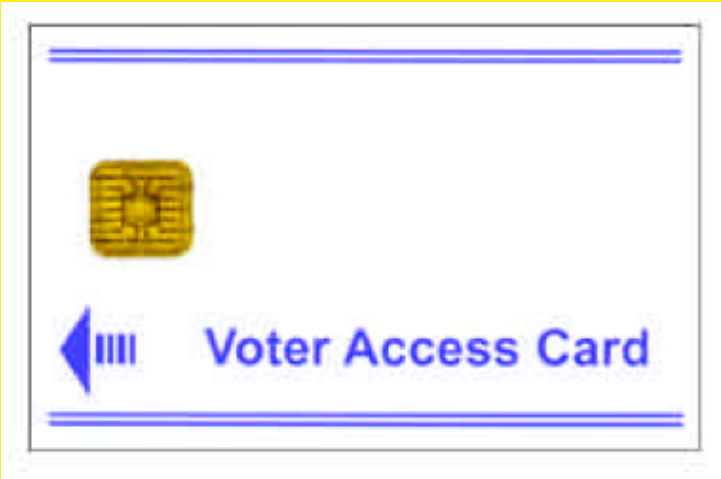
- Tests conducted with help of Maryland SBE
- Group assembled and led by Mike Wertheimer, RABA Technologies
  - Very talented group of security analysts
  - Asked us to play attacker
  - Set up a "precinct" and "local board of elections" server
  - One week to study everything, one day to attack

What We Found

- Not good
- Procedural controls can mitigate many problems on a short-term basis
- System needs major overhaul from the security perspective

Smart Cards

- Supervisor, voter access ,security key cards are same model



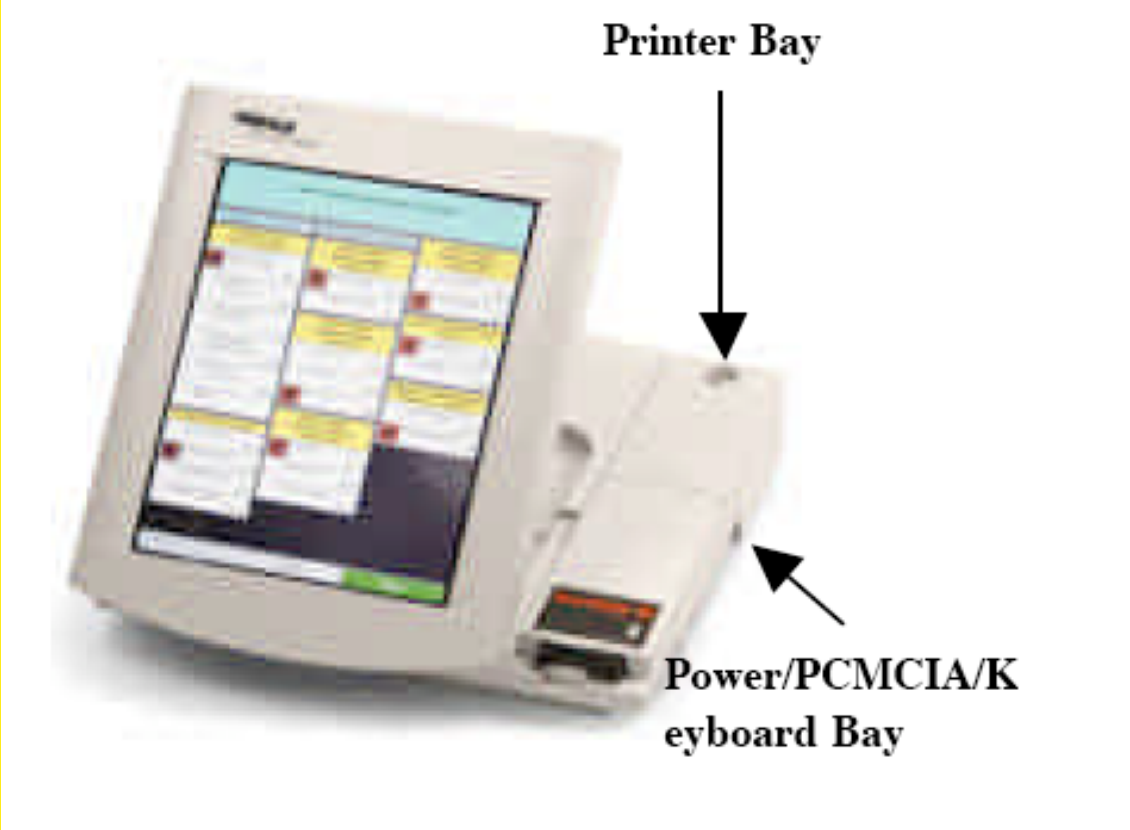
Compromise

- Information on cards password protected
  - Passwords easy to guess, turned out to be same as Hopkins study reported (!)
- Given contents, easy to:
  - Duplicate
  - Change type of card
  - Reinitialize voter card

Recommendations

- Make passwords be on a per-precinct basis, and automatically generated using security key cards
- Procedures to prevent use of unauthorized supervisor cards

AccuVote-TS Terminals



Compromise

- All locks have the same key
  - Can duplicate it in any hardware store
  - Pick locks in under 1 minute (first timer), 10 seconds (with some knowledge)
- In bay lie PCMCIA card, PS2 port
  - Hook up keyboard, hit F2 or Enter and you're a Supervisor!
- Jam card reader
- Disconnect monitor

PCMCIA Cards

- Install new passwords
  - Terminal needs to be reset before it can be used
- Remove PCMCIA card, substitute one with names switched on ballot
  - Votes recorded by position on official ballot, not by name
- Update the software
  - Can change the ballot

Recommendations

- Secure bays with tamperproof tape with serial numbers, both inside and out
- Delete test recording software from terminal
  - Blocks keyboard attack
- Legal methods to deter tampering with hardware (like monitor, card reader)

Server

- Assumed limited physical access (5-30 min), phone access via modem
- Assumed not connected to Internet or local area networks
- Focused on access through modem

Compromises

- 15 patches behind
  - Took over using same exploit Blaster used (patch available since July 16, 2003)
    - Upload, download, execute files with Administrator privileges
  - Off-the-shelf exploit did this one

Physical Access

- Insert CD that uploads malicious code, modifies or deletes ballots and/or data, reorder ballot definitions
- Insert CD, boot
  - Note: database files containing votes are *not* encrypted not signed
- Stick a USB flash drive in USB port in rear of machine
  - Now upload malicious software to system

Remote Access

- Man-in-the-middle attack
  - Persuade precinct to call your laptop, get results, modify them, then you upload them to LBE
    - You get name, password in download
    - SSL used, but it's incomplete: no authentication!
- Modify election database
  - Audit logs are in there, too

Recommendations

- Patch and secure the server
- Procedures for minimizing phone problems
- Disable CD autorun feature
- Physically secure server
- Boot order should be HD, then CD, and BIOS should be password protected

Paper Receipts

- Consensus was they were needed, but not on all systems
  - Pick one or two in each precinct, have them print out votes, and at end of day reconcile—if the counts match, should be fine
  - In case of error, do a revote
    - There is precedent for doing it in Maryland (for which the report was written)
    - *Very* cumbersome approach!
    - This may not be possible in other jurisdictions …

Conclusions

- Best way to use e-voting machines:
  - Print paper ballots
  - Count paper ballots
- If you must use them to count votes:
  - Print paper ballots for each vote as cast, and have voters verify them
  - Use system like the 1% law in California to validate the system's integrity

Diebold's Response

Maryland Security Study Validates Diebold Election Systems Equipment for March Primary

Findings Consistent With Prior SAIC Review

Today, the Maryland Department of Legislative Services, based on the analysis by RABA Technologies, concludes that the March primary election can be held successfully without any changes to the Diebold Election Systems software. The software accurately counts votes cast and has the ability to render a printed image of every ballot cast in the event a recount is necessary.

"The findings in the SAIC and RABA reports both confirm the accuracy and security of Maryland's voting procedures and our voting systems as they exist today," said Bob Urosevich, president of Diebold Election Systems, Inc. "With that said, in our continued spirit of innovation and industry leadership, there will always be room for improvement and refinement. This is especially true in assuring the utmost security in elections."

— *Diebold Press Release, January 29, 2004*