CS 155 June 1, 2004

Electronic Voting

Dan Boneh John Mitchell

Issues

- Voting system security requirements
  - Secret ballot, reliable counting, voter anonymity, …
- Voting technology
  - History: Paper ballots, lever machines, …
  - Direct Recording Electronic (DRE) systems
- Case studies
  - Diebold case study
  - Internet voting (retracted by gov't)
- Cryptographic approaches
- Politics
  - Voting Rights Act bills H.R. 3295 and S. 565
  - California Secretary of State Kevin Shelley
  - IEEE Standards committee

Voting Principles

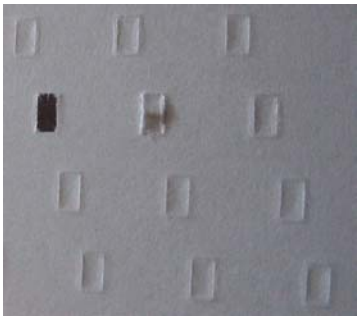
- Voter eligibility
  - No voter should have more than one vote
- Secret Ballot
  - Votes cast in secret
  - Voter should be confident that vote cast correctly
- Reliable counting
  - Public system, typically with officials from all parties
  - Ability to recount
    - Some election officials may prefer not to do this
- Anonymity
  - Voter should not leave voting booth with any proof of the way he/she voted

Recent History

- 2000 Presidential Election
  - Hanging chad, contested absentee votes
- Help America Vote Act (HAVA, HR 3295, Oct 02)
  - Mandates voting process reform in all states
  - Voters must be able to verify ballots before they are cast
  - "permanent paper record with a manual audit capacity"
  - voter must have "opportunity to change the ballot or correct any error before the permanent paper is produced"
- Electronic voting
  - Touchscreen, Direct Recording Electronic (DRE) systems
  - Proponents argue HAVA requirements are met if the voter verifies a screen version of the ballot, and if a paper report can be printed later for audit purposes

Punch card device

Punched card



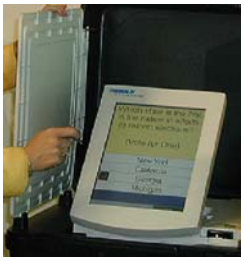
Other alternatives

- Mechanical lever machines
  - Voter flips mechanical levers
  - Machine reports votes
  - Tamper-proof counter similar to car odometer
- Optical scan of paper ballots
  - Like our teaching evaluations …
  - Fairly reliable counting method
  - Requires pencil and paper ballots

Lever machine

Touch-screen voting

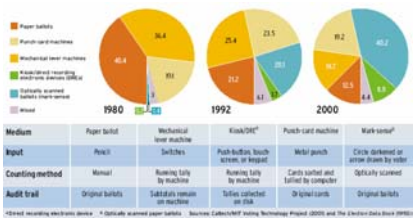
- Usability
  - Customized ballot
  - Easy to read, vote
  - Accessible to blind
    wear headphones
- Vote counting
  - DRE system provides quick count
- Voter "authentication"
  - smartcard reader (lower-right corner)



Diebold AccuVote-TS

http://www.sos.state.ga.us/

How votes are cast



	1980	1992	2000
Medium	Paper ballot	Kiosk/DRE*	Mark-sense*
Input	Pencil	Push-button, touch screen, or keypad	Circle darkened or arrow drawn by voter
Counting method	Manual	Cards sorted and tallied by computer	Optically scanned
Audit trail	Original ballots	Original ballots	Original ballots

IEEE Spectrum
Oct 2002

Problems with electronic voting

- Washington Post 11/6/2003
  - Software glitch in November's election in Virginia
  - Advanced Voting Solutions touchscreen machines
  - "Voters in three precincts reported that when they attempted to vote for [Thompson], the machines initially displayed an 'x' next to her name but then, after a few seconds, the 'x' disappeared. In response to Thompson's complaints, county officials tested one of the machines in question yesterday and discovered that it seemed to subtract a vote for Thompson in about 'one out of a hundred tries,' said Margaret K. Luca, secretary of the county Board of Elections. "

    http://www.washingtonpost.com/wp-dyn/articles/A6291-2003Nov5.html
- Indianapolis Star 11/9
  - Software glitch in November's election
    - 19,000 registered voters
    - 144,000 votes tallied
    - actual number of votes cast was 5,352
  - MicroVote touchscreen machines

    http://www.indystar.com/articles/6/091021-1006-009.html

Voter Verified Audit Trail

IEEE Spectrum
Oct 2002

Case Study: Diebold machine

T. Kohno, A. Stubblefield, A. Rubin, D. Wallach

Basis for study

- Proprietary system
  - Certification mandated by election laws
    - Without public review: Security through obscurity
- Diebold system leaked
  - AccuVote-TS DRE voting system, Oct 2000 - April 2002
  - Available on open ftp server
  - Identified by activist Bev Harris
  - Some zip files, cvs repository
    - DMCA concern over zip "encryption"
    - Available on New Zealand site
- No access to Diebold's back-end election management system

Some problems

- Encrypted votes and audit logs
  - 56-bit DES in CBC mode with static IVs
  - #define DESKEY ((des_key*)"F2654hD4")
  - Unkeyed public function (CRC) for integrity
- No authentication of smartcard to voting terminal
- Insufficient code review

Sample comment in code

```
//  LCG - Linear Conguential Generator
//  used to generate ballot serial numbers
//  A psuedo-random-sequence generator
//  (per Applied Cryptography,
//  by Bruce Schneier, Wiley, 1996)
```

Unfortunately, linear congruential generators cannot be used for cryptography"

Page 369
Applied Cryptography, by Bruce Schneier

- BallotResults.cpp
Diebold Election Systems

Other examples

"this is a bit of a hack for now."
AudioPlayer.cpp

"the BOOL beeped flag is a hack so we don't beep twice. This is really a result of the key handling being gorped."
WriteIn.cpp

"the way we deal with audio here is a gross hack."
BallotSelDlg.cpp

"need to work on exception *caused by audio*. I think they will currently result in double-fault."
BallotDlg.cpp

Code Fragment

```
void CBallotRelSet::Open(const CDistrict* district, const CBaseunit* baseunit,
const CVGroup* vgroup1, const CVGroup* vgroup2)
{
  ASSERT(m_pDB != NULL);
  ASSERT(m_pDB->IsOpen());
  ASSERT(GetSize() == 0);
  ASSERT(district != NULL);
  ASSERT(baseunit != NULL);
  if (district->KeyId() == -1) {
    Open(baseunit, vgroup1);
  } else {
    const CDistrictItem* pDistrictItem = m_pDB->Find(*district);
    if (pDistrictItem != NULL) {
      const CBaseunitKeyTable& baseunitTable = pDistrictItem->GetBaseunitTable();
      int count = baseunitTable.GetSize();
      for (int i = 0; i < count; i++) {
        const CBaseunit& curBaseunit = baseunitTable.GetAt(i);
        if (baseunit->KeyId() == curBaseunit.KeyId()) {
          const CBallotRelationItem* pBalRelItem = NULL;
          while ((pBalRelItem = m_pDB->FindNextBalRel(curBaseunit, pBalRelItem))){
            if (!vgroup1 || vgroup1->KeyId() == -1 ||
                (*vgroup1 == pBalRelItem->m_VGroup1 && !vgroup2) ||
                (vgroup2 && *vgroup2 == pBalRelItem->m_VGroup2 &&
                 *vgroup1 == pBalRelItem->m_VGroup1))
              Add(pBalRelItem);
          }
        }
      }
      m_CurIndex = 0;
      m_Open = TRUE;
    }
  }
}
```

Zero Comments

Other problems

- Ballot definition file on removable media unprotected
- Smartcards use no cryptography
- Votes kept in sequential order
- Several glaring errors in cryptography
- Inadequate security engineering practices
- Default Security PINs of 1111 on administrator cards
- Windows Operating System
  - tens of millions of lines of code
  - new "critical" security bug announced every week

Insider threat

- Easy to hide code in large software packages
- Virtually impossible to detect back doors
- Skill level needed to hide malicious code is much lower than needed to find it
- Anyone with access to development environment is capable
- Requires
  - background checks
  - strict development rules
  - physical security

Insider Example

- Rob Harris case - slot machines
  - Worked for Gaming Control Board
- Malicious code in testing unit
  - when testers checked slot machines
    - downloaded malicious code to slot machine
  - was never detected
  - special sequence of coins activated "winning mode"
- Caught when greed sparked investigation
  - $100,000 jackpot

Another insider example

- Breeder's cup race
  - Upgrade of software to phone betting system
  - Insider, Christopher Harn, rigged software
  - Allowed him and accomplices to call in
    - change the bets that were placed
    - undetectable
  - Caught when got greedy
    - won $3 million

Other Studies

- SAIC report
  - 2/3 of the report redacted
  - Executive summary:
    "The system as implemented in policy, procedure, and technology, is at high risk of compromise."
- Ohio report
  - Cited "critical flaws" in top 4 vendors' voting machines
- RABA report
  - ex-NSA red team consulting company
  - Executive Summary:
    - "The State of Maryland election system (comprising technical, operational, and procedural components), as configured at the time of this report, contains considerable security risks that can cause moderate to severe disruption in an election."

Diebold response

- Press release headline:
  - "Maryland Security Study Validates Diebold Election Systems Equipment for March Primary: Findings Consistent With Prior SAIC Review"
- Company President:
  - "Touch screen voting from Diebold Election Systems has evolved to be the most secure and accurate election system in the history of our democracy."

Recommendation #1

- Separate vote casting from tabulating
  - Touch screen machine produces paper ballot
    - need not be as trusted as today's DREs
  - voter can use or destroy
  - scanning and tabulating machine
    - small code base
    - open source
    - extensive testing and certification
    - different manufacturer from touch screen

Recommendation #2

- Transparency
  - Require designs of machines to be public
  - Require security audit of machines by qualified experts
    - Require public report of this audit
  - Require open source for vote tabulation code
    - necessary but not sufficient

Recommendation #3

- Quality control
  - Establish criteria for testing the expertise of manufacturers
    - NIST could play this role
  - Require source code analysis for certification
  - Establish standards for policies and procedures
    - Aim for simplicity:
      - The more complicated and burdensome, the less likely to be followed

SERVE

- Built by Accenture for FVAP
- Participating states
  - Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington
  - 50 counties
- Military and overseas civilians
- Use *any* PC anywhere
  - running Windows
  - running IE or Netscape
- Formed SPRG
  - two 3-day meetings, design/review/demo

Key security concerns

- Insecure platform
  - trojan horses, viruses, worms
  - malicious hijacked system
    - in cyber café
    - at neighbor's house
    - roaming laptop
- Denial of Service attacks
  - just look at MyDoom attacking SCO
  - 30 day window, but most people vote on last day
- Phishing/man in the middle attack
  - especially effective against privacy
  - allows automated vote selling

San Jose Mercury Thu, Apr. 22, 2004

The controversy continues …

E-voting panel wants to dump troubled system

By Elise Ackerman
Mercury News

SACRAMENTO - Less than seven months before the presidential election, an advisory panel Thursday unanimously recommended an unprecedented ban of touch-screen election equipment used in four California counties.

The panel also urged Secretary of State Kevin Shelley to seek a criminal or civil investigation into the conduct of Diebold Election Systems, the Ohio-based firm that manufactured the troubled voting system.

San Jose Mercury Sunday May 30, 2004

Lax controls over e-voting testing labs

ELECTION OFFICIALS RELY ON PRIVATE FIRMS
By Elise Ackerman
Mercury News

California Secretary of State Kevin Shelley had a simple question: Had a new electronic voting machine been approved by an independent testing lab?

State law requires such approval before the device could be used by California voters. …

Wyle Laboratories of El Segundo refused to discuss the status of its testing of the AccuVote-TSx machine made by its client, Diebold Election Systems. The information was proprietary, Wyle said, and could be revealed only to Diebold.

Summary

- No one knows how to build bug-free systems
  - Need public review, testing, redundancy
- Insider attacks are possible
- Voter-verifiable audit trail gaining popularity
  - CA Secretary of State Kevin Shelley
    - Banned Diebold TSx voting system from the state
    - Decertified all electronic voting until certain conditions can be met by either the vendors or the Counties
    - "I want to state clearly and unequivocally: there will be a paper trail for every single vote cast in the state of California, and it will happen on my watch."

http://www.verifiedvoting.org/

Verifiable Voting Technology

- Three methods:
  1. Mix Nets (Chaum '81)
     - Two types: onion mix net, re-encryption mix net.
     - VoteHere – Re-encryption mix net product.
     - Chaum – Based on visual cryptography
  2. Homomorphic encryption.
     - Based on encrypted counters.
     - Difficulty with complex ballots and write-ins.
  3. Blind signatures
     - Not often used due to weak auditing features.

Onion Mix Net voting system

- Components and participants:
  - Voters.
  - Vote input station + vote collection station.
  - Mix servers (e.g. 5 servers)
  - Election officials.
- Setup:
  - Each mix server generates a public/private key pair:
    PK_{MSi} , SK_{MSi} i=1,...5,
  - All public keys PK_{MS1}, …, PK_{MS5} are stored in voting sation.

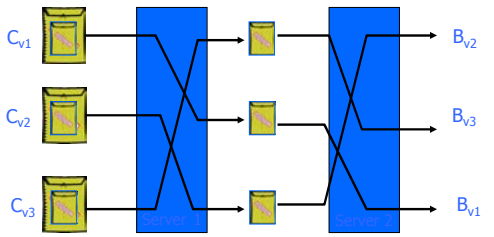
Casting vote

- Voter V walks up to vote input station and fills out his/her ballot B_v .
- Vote input station prepares ciphertext:

  $C_v = E_{PK_{MS1}}[\, E_{PK_{MS2}}[\, \ldots [\, E_{PK_{MS5}}[\, B_V \,]] \ldots \,]]$
  - Gives voter receipt (voter-name, C_v).
  - Voter gives copy of C_v to vote collection station.
- How can voter tell that C_v contains right ballot?
  - Possible answer: election officials create ballots throughout day and test resulting C_V's by decryption.

Mixing

- Desired effect: shake ballot box



Notes

- Integrity:
  - Each server also outputs proof that output is a permutation + decryption of input.
  - At end of election voter V checks:
    - C_v entered the mix net, and
    - All proofs output by mix server are correct.
  - Voter is assured his/her vote was counted.
- Privacy:
  - Suffices that 1-of-5 mix servers creates a random permutation and keeps it secret.

Notes

- ◆Anonimity:
  - voter cannot prove to 3rd party how he voted.
  - Caveat: covert channel based on ballot complexity.
- ◆Problem: robustness
  - If one mix server crashes/defects votes cannot be decrypted.
  - One solution: share mix server decryption keys among election officials.
  - Better solution: re-encryption mix net.

Re-encryption mix net

- ◆Need public key system supporting re-encryption.
  - Given $C = E_{PK}[M]$ anyone can create new random encryption of M under PK.
  - Example: ElGamal encryption.
- ◆Setup:
  - Election officials generate a public $PK_{election}$.
  - Corresponding private key shared among them: all (or most) officials needed to decrypt.

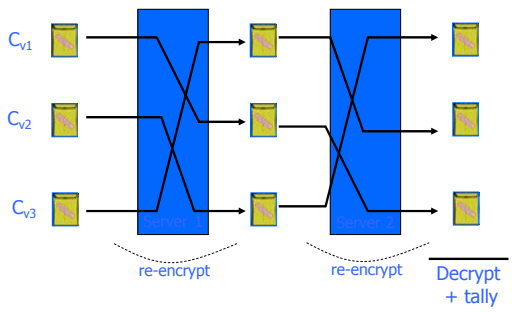
Casting vote

- ◆Voter V walks up to vote input station and fills out his/her ballot B_v .
- ◆Vote input station prepares ciphertext:

$$C_v = E_{PK}[B_V]$$

  - Gives voter receipt (voter-name, C_v).
  - Voter gives copy of C_v to vote collection station.

Mixing



Notes

- ◆Integrity and privacy as before.
  - Servers output proof that re-encryption preserves integrity
    (i.e. output is permutation of input)
  - Integrity is guaranteed.
    Privacy depends on randomness from servers.
- ◆Robustness: no harm if few servers crash.
- ◆VoteHere: uses Neff mix net.
  - Based on ElGamal re-encryption.
  - Provides efficient integrity proof.

Voting using Hom. Encryption

- ◆Homomorphic encryption:
  - Public key system such that given
    $C = E_{PK}[M]$
    anyone can create $C' = E_{PK}[M+1]$
- ◆Example: public key: $N=pq$, g
  private key: p, q

  $E_{PK}[m] = g^m r^N \pmod{N^2}$
- ◆Then: $C = E_{PK}[m] \Rightarrow C' = C \cdot g \cdot (r')^N \pmod{N^2}$

Election

- Setup:
  - Election officials generate PK/SK for hom. enc. system.
  - For each candidate P_i generate $C_{P_i} = E_{PK}[\ 0\ ]$
  - Voting station: $[\ C_{P_0}\ ,\ C_{P_1}\ ,\ \ldots\ ,\ C_{P_n}\ ]$
- Each voter walks up to voting station:
  - Randomizes all ciphertexts
  - Adds one to one of the ciphertexts.
  - Proves that only one counter changed and changed by 1.
- End of day:
  - Officials decrypt all counters to get tally.

Summary

- Mix nets provide a mechanism to address many voting requirements:
  - Privacy, integrity, verifiability, anonymity.
  - Difficulty: must ensure that vote input station creates correct ballot.
  - Integrity proofs are not easily understood by non-cryptographers.
  - Main challenge: simple & easy-to-understand mix net.
    - Some success: Jackobsson-Jules-Rivest
- Homomorphic encryption:
  - Limited utility: can only implement elections based on straight vote counting. No write-ins.