A special case: Diebold AccuVote -TS

- In January 2003 Bev Harris stepped accidentally on a web-site holding some 40.000 files including user manuals and source code for voting machines
- Usually source code of voting machines is proprietary and therefore kept secret
- Unique opportunity for a rigorous analysis of a widely used electronic voting system
- Opportunity to validate adequacy of standards
- Version numbers of Diebold code certified by NASED are closely related to those examined by Hopkins group (p10, Jones, Diebold case)

Diebold AccuVote -TS

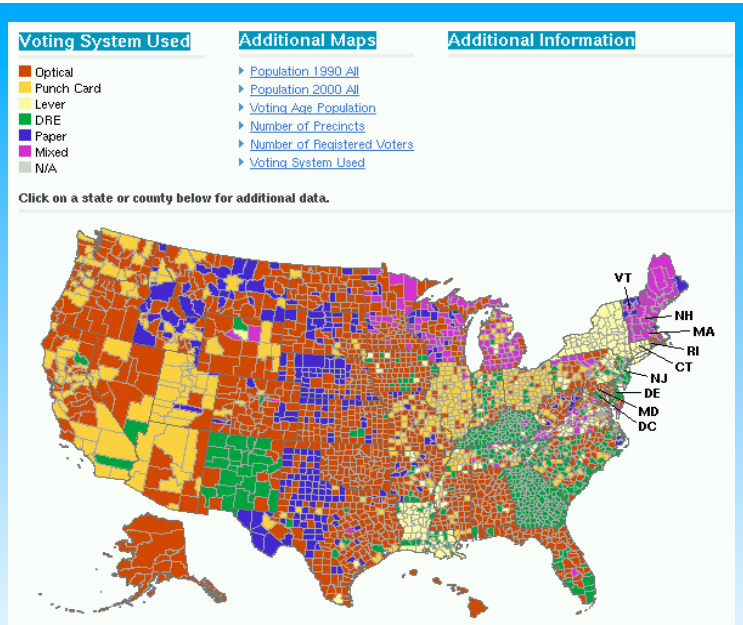
Two main components:

- GEMS voting server
  - GEMS software for communication with voting terminals to load ballots and transfer voting results
- Direct Record Entry (DRE)
  - touch screen,
  - active memory component with OS, ballot information, temporary record of votes
  - PCMCIA flash memory card containing votes
  - internal ribbon printer and optional audio component
  - support for modem connection

Direct Recording Entry

- Example of a voting booth for DRE: Electrovote 2000 (Fidlar)
- Offers much less privacy than the voting booths currently used in e.g. Italy and the Netherlands.

Picture: D.W. Jones



From: Election Data Services, map of January 2003

The controversy (CRS2003)

- Vendors and election administrators claim that:
  - Current measures taken to guarantee security of electronic voting machines are enough
  - Those who criticize the current voting machines have not enough understanding of how voting systems work and how elections are administered (i.e. procedural aspects)
- Computer experts and some activists claim that:
  - Current measures are not sufficient
  - Elections should rely on openness, transparency and observability of the whole election process in order to guarantee security (i.e. no blind trust)
  - Election system should be Voter and Results Verifiable

What are the exact problems?

The Diebold case is unique because it is the only commercial system of which, inadvertently, a software version has become public

- Why use of Third-party software is a problem?
  - Independent certification commissions
  - Self-modifying code and dynamic linking
- How secure is the communication of results?
  - Communication from DRE to the central office
- What are the effects of (malicious) system shut down?
- Why is a good accounting system important?

Confirmed by Maryland 2004 report reviewing Diebold system

Sources: D.W. Jones[J], Rubin report[R], SAIC report[S], Maryland 2004[M]

Third-party Software

- Many electronic voting systems use COTS: commercial 'of-the-shelf' software which is proprietory (closed for public scrutiny)
- E.g. AccuVote-TS uses a version of Windows and various Microsoft Office components. If this code is used unmodified then it is not subject to source code audit under FEC/NASED rules [Jones]
- But: such software must be documented (i.e. version number, vendor etc.) and upgrades re-certified
- It could contain self-modifying code and dynamically linked libraries

Self-modifying code

- Two definitions:
  - "machine instructions that are overwritten by other instructions at run-time"
  - "any use of dynamic linking or interpretative execution which can be used to change the function of the programming code"
- Makes it extremely difficult to detect correctness of the code and to detect whether malicious computer code has been introduced
- MS Windows makes extensive use of dynamically linked libraries and Visual Basic interpreters

Security problems

Several security problems have been identified:

- Unauthorised access
- Risk of changes during transport of votes
- Problems in counting procedures
- Risks of connections to the Internet/modem and wireless connections

We give some examples of each of them

Security problems in the voting booth

Unauthorized access to DRE

- Smart-cards do not perform any cryptographic operations and could be 'reverse engineered' to get unauthorized access to DRE. Potential consequences:
  - Multiple votes issued
  - Provoke premature shutdown of election machine and voters may not come back later when the machine is substituted
- Lack of defense against unauthorized access by election insiders
  - No logs of changes made by insider personnel

Security problems with vote transport

After the polling places close, the votes on the DRE have to be consolidated at the precinct and then transported to the central offices where the precinct reports may be tabulated and printed using the GEMS software

Main weaknesses identified:

- data on PCMCIA cards
- transport 'by hand' or via modem
- in software found at ftp-site the encryption key was hard-coded into the source code

PCMCIA cards for voting data

- Example of the size of a ballot module (Nedap)

Risks:

- Very small size: possibility that modules get exchanged or reprogrammed unnoticed

Despite separation of DRE from network:

- data needs strong encryption
- authentication of module
- verification integrity of data

Transport of data (to precinct)

Several methods used for transport of voting data:

- Via the Internet (nowadays avoided, no total security can be guaranteed)
- Via modem connection after closure of elections for preliminary unofficial results only
  (Diebold, for vote totals)
- "by hand" transport of ballot module to precinct (Diebold, Nedap)

Encryption key management

- Security of PCMCIA cards requires the same level of care as security of network transmission, however:
- The SBE does not require encryption for the unofficial election results transmitted electronically from the local polling sites to the LBE
- All data on the storage device is encrypted using a single, hardcoded DES key. If the key is discovered, this could be used to alter data in several polling places, and probably also in subsequent elections
- Multiple keys are needed and a well-defined key distribution protocol

"Social engineering" attacks

- Exploitation of people's weaknesses, e.g.:
  - premature publication of intermediate results (people may be induced to vote for the most likely 'winner')
  - temporary unavailability of machines may create long waiting lines, inducing people not to vote
  - Man in the middle attack during votes transport by modem may lead to large difference in unofficial and official outcome of election results -> damages trust
- Provoking premature shutdown of "critical" polling sites
- Most weaknesses were of this kind in Maryland study (= SAIC report)

Need for good accounting system

- Fraud needs to be detectable
- Recovery from errors, fraud or malfunctions
- Possibilities for independent recounts

Proposals to resolve the controversy

(CRS Nov. 2003)

- Use current procedures
- Improve Security Standards and Certification
- Use Open Source Software
- Improve Verifiability and Transparency:
  - Voter-verifiable Paper Ballot
  - Votemeter
  - Modular Voting Architecture
  - Encrypted Votes

Use current procedures

- Mainly supported by vendors of equipment
- Security must come mainly from good procedural rules that have to be followed by everyone involved in organising the elections
- Requires much expensive training of officials
- No guarantees about correctness of software
- Difficult to evaluate effectiveness

Improve Security Standards and Certification

- VSS standard voluntary, not following best practices, marginal involvement of ANSI, ISO, NIST
- Current certification of Diebold software has not revealed problems detected later by experts
- Improvement of VSS is in progress under EAC in collaboration with ANSI, IEEE, NIST, NASED
- Standards cannot deal with unforeseen threats, are time-consuming to develop but may provide guidelines for avoiding design flaws
- Does not resolve transparency issue

Use Open Source Software

- Software available for public inspection
- Potentially more thorough security check possible
- Potential flaws may also be easier to discover and to exploit by criminals
- Current DRE software is based on/contains proprietary software
- Proposed solution: separate software for the user-interface from that of the vote-casting/counting. E.g. touchscreen producing ballot that can be put into separate optical scanner (latter open source)

Improve Verifiability and Transparency

- Voter verifiability: voter can check whether vote has been cast as intended
- Results verifiability: final tally faithfully reflects all votes as cast by the voters
- Both possible with paper ballots only if accurate observation of counting is performed
- None possible with lever-machines and electronic voting machines
- Partially possible with punch-card and optical scan
- Need observable ballots that can be recounted

Voter-verifiable Paper Ballot

- DRE prints paper ballot of voter's choices
- Voter can check, but not touch ballot
- Ballot is stored separately in ballot box for sample counting or for recount
- Paper ballots should maybe be counted by hand

Voter-verifiable Paper Ballot

Potential advantages:

- recount on independent voter verified record
- auditing of election possible
- recount by hand restores transparency
- could restore confidence in legitimacy of election

Critics:

- voting for voter is (slightly) more complicated
- printers could break down and cost more
- paper ballots cannot satisfy accessibility requirements
- not tested yet, impact unclear
- hand counting is time-consuming

Votemeter

- Separate module that counts votes electronically but independently from DRE
- Makes audits possible
- Needs trust of voters on fact that the modules operate indeed separately
- Full audit can take place fast and independent
- No problems with accessibility requirements

Modular Voting Architecture

- Separate user-interface from vote-counting
- Voter transfers vote from DRE to counting device by means of a memory-card (frog)
- Needs security of memory-card
- Issues similar to preceding option

Encrypted Votes [D. Chaum]

- Clever use of cryptographic techniques
- Completely electronic
- Claim is that voters can verify whether their vote has been counted as casted without compromising vote secrecy (zero-knowledge proof protocol)
- Unpublished manuscript as for now
- Needs more time to be developed
- Theory may not be easy to explain to voters, so confidence may be compromised

Electronic systems in practice

- Nov. 2003, the Mississippi Senate declares election invalid. The WINnVote touchscreen machines had trouble starting up, many overheated and went out of service, many voters left without voting due to long delays [Risks, Vol. 23(19)]
- March 2, 2004 in random 1% recount it was found that an optical-scan of paper absentee ballots failed to record votes on some ballots. 11,000 ballots were re-scanned, problem due to calibration. Detected due to recount possibility. [Risks, Vol.23(2)]

Electronic systems in practice

- March 2, 2004 in 17 counties in California in which Diebold systems were used, none of the versions of those systems actually used was the version that had been certified [Risks, Vol. 23(2)]
- April 30, 2004, California Secretary of State Kevin Shelley announced de-certification of all electronic touch-screen voting machines in the state due to security concerns and lack of voter confidence. [Risks forum, May 4, 2004, Vol. 23(35)]
- November 12, 2003, in Boone County election using MicroVote software, the system returned 144.000 votes with only 19.000 registered voters [Risks, Vol (23)3]

Electronic systems in practice

- November 2002, Wake county, North Carolina 436 ballots were lost using ES&S iVotronic touch screen machines. Discovered accidentally, because absentee ballots were acquired of all people voting that day on the TS machine. ES&S admitted that the problem was caused by flawed software. [Voter Verification Newsletter, Vol. 2(3)]
- January 2004, Florida, 134 blank ballots cast on iVotronic machine [VVN, Vol. 2(3)]

Electronic systems in practice

- November 8, 2003, in Alameda county someone working for Diebold had access to the TS machines used in the election to make unauthorized changes to the vote-counting software [Risks, Vol 23(3)]
- February 2004, a computer security expert hired by Maryland's legislative services department managed without much effort to enter Diebold system both from inside as well as via remote dial in. [VVN, Vol. 2(3)]

Electronic systems in practice

- November 4, 2003, Fairfax County using AVS touch screen voting systems discovered that marks indicating a vote disappeared after a few seconds resulting in votes not being recorded. This caused Rita Thompson loosing a close race loosing approximately 1 every 100 cast votes due to this error. [VVN, Vol 1(13)]
- 2004 ongoing investigation of many reports on problems with the voting system during the 2004 Presidential Election

Electronic Voting Machines

- Main advantages:
  - Short time between voting and results
  - Expected reduction of errors in counting procedure
  - Huge reduction in use of paper
  - Flexible adaptation to user's special needs
  - Flexible configuration of ballots
  - Expected reduction in cost (personnel and other)

Electronic Voting Machines

- Main disadvantages (with current machines):
  - Voter is forced to rely on `blind trust': voting software is in almost all cases proprietary and software sources are not available for public scrutinity.
  - Use of third party commercial software
  - Complete security of a computer system is very hard to guarantee and to obtain and unauthorized access may lead to many votes being changed undetected
  - Lack of audit trails that can be verified also by non-experts in case recounts are believed necessary