University of Connecticut VoTeR Center

Voting Technology and Election Integrity: Landscape and Challenges

Alexander Shvartsman

UCONN Center for Voting Technology Research

aas@cse.uconn.edu

Electronic Voting Machines

- Why?
  - Smaller error-rates in counting
  - Improve access for disabled citizens
  - Flexible interfaces
  - Reduce ambiguity for voters
  - Eliminate/reduce overvoting and undervoting
  - Precision

Voting is a hard problem

- Voter registration – each eligible voter is able to vote, and votes at most once
- Voter privacy – no one can tell how any voter voted, even if voter wants it; no “receipt” for voter
- Integrity – votes can’t be changed, added, or deleted; tally is accurate.
- Availability – voting system available when needed
- Ease of use & Accessibility – voters with disabilities
- Assurance – verifiable integrity

Electronic Voting Machines

- How hard can it be to do +1 anyway?
- And who could possibly object to modernizing?
  - Luddites?
  - Computer Science Theoreticians?
  - Other Nay-Sayers?
- We all use bank ATMs, right?
  - Why not electronic voting machines?

Outline

- Some history and motivation
- Scope: integrity of extant onsite voting
- Overview of technology and issues
- Security issues – how real are they?
- Case studies in security
- What technologists can do?
- Closing thoughts

Center for Voting Technology Research

- 2005-2006 Member of the State of Connecticut Voting Technology Standards Board
- 2006 Work with Connecticut CFP Committee
- 2006+ Partnership with the CT SOTS Office
  - Advising on the voting technology issues
  - Evaluation and safe use of voting equipment
  - Design and implementation of technological audits
  - Contributions to hand-counted audits
- Publications http://voter.engr.uconn.edu

VoTeR Center Staff

- Alex Shvartsman, Director
- Principal Investigators:
  Aggelos Kiayias, Laurent Michel, Alex Russell
- Research Faculty: Suzanne Stark
- Staff Researcher: Tigran Antonyan
- Assistants:
  - Graduate assistants:
    S. Davtyan, L. Nazaryan, J. Neumann
  - Undergraduate students: R. Jancewicz, E. Kovalev
  - Debra Mielczarek, Administrative Assistant
  - Other graduate/undergraduate students in the past

VoTeR Center Capabilities

- Voting technology expertise
- Dependability and fault-tolerance
- Security and cryptography
- End-to-end security analysis
- Black-box analysis voting systems
- Hands-on analysis of voting equipment hardware
- Design of software for security evaluation
- Pre-election and post-election technical audits
- Audits and analysis

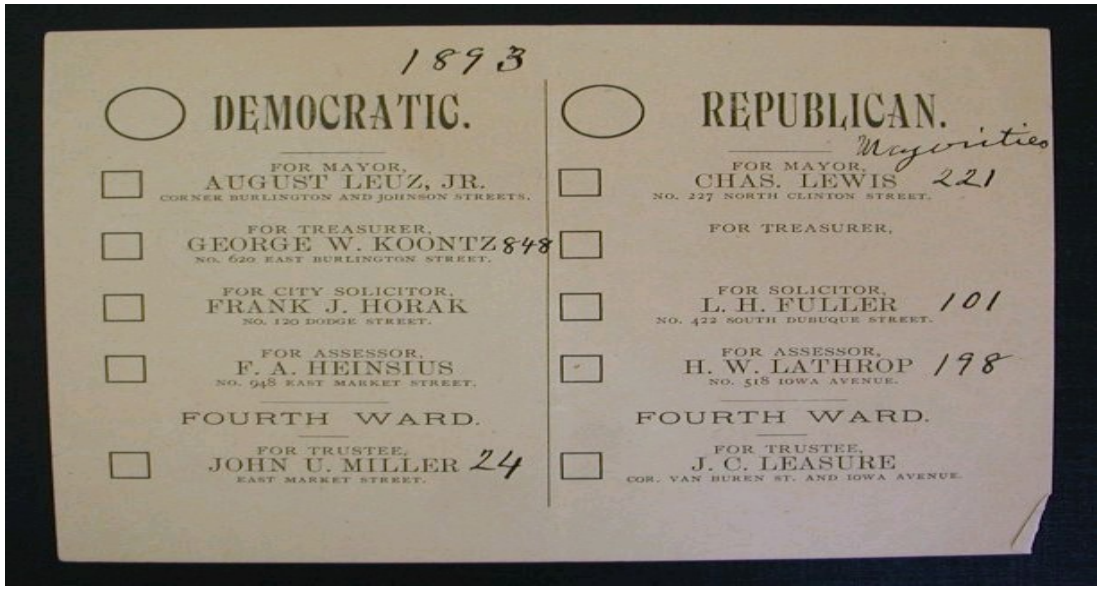
Voting Equipment Evaluation

- Activity since Spring 2006
- VoTeR Center evaluated several systems
  - AccuVote Optical Scan system
  - IVS Inspire vote-by-phone system
  - Others (NDA)
- The evaluations are done in the UConn VoTeR Lab
  - Black-box evaluation & in-depth hardware/software analysis
  - Exploration of possible attack vectors
  - Physical integrity
  - Mitigation strategies and safe use recommendations

Accomplishments & Current Focus

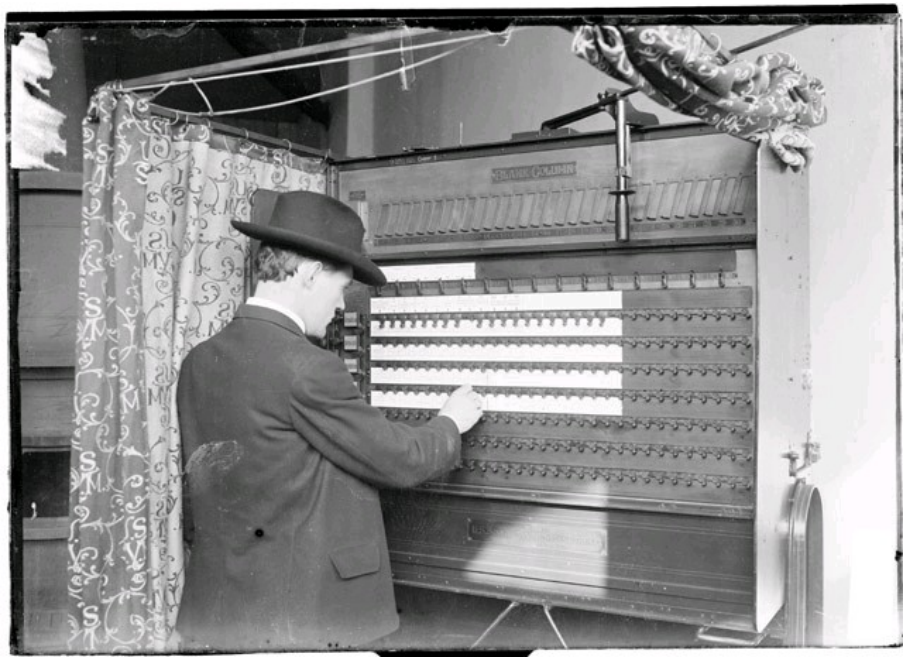
- Security analysis of AccuVote Optical Scan
- Threat vector assessment and design
- Safe use procedure recommendation
- Assistance with audit design and analysis
- Complete analysis of memory cards
- Reverse-engineering of firmware and protocols
- Assessment of software/firmware upgrades
- Precision evaluation and analysis
- Technology / issue tracking

Paper Ballots



- Lincoln ballot, 1860, San Francisco
- “Australian ballot”, 1893, Iowa city

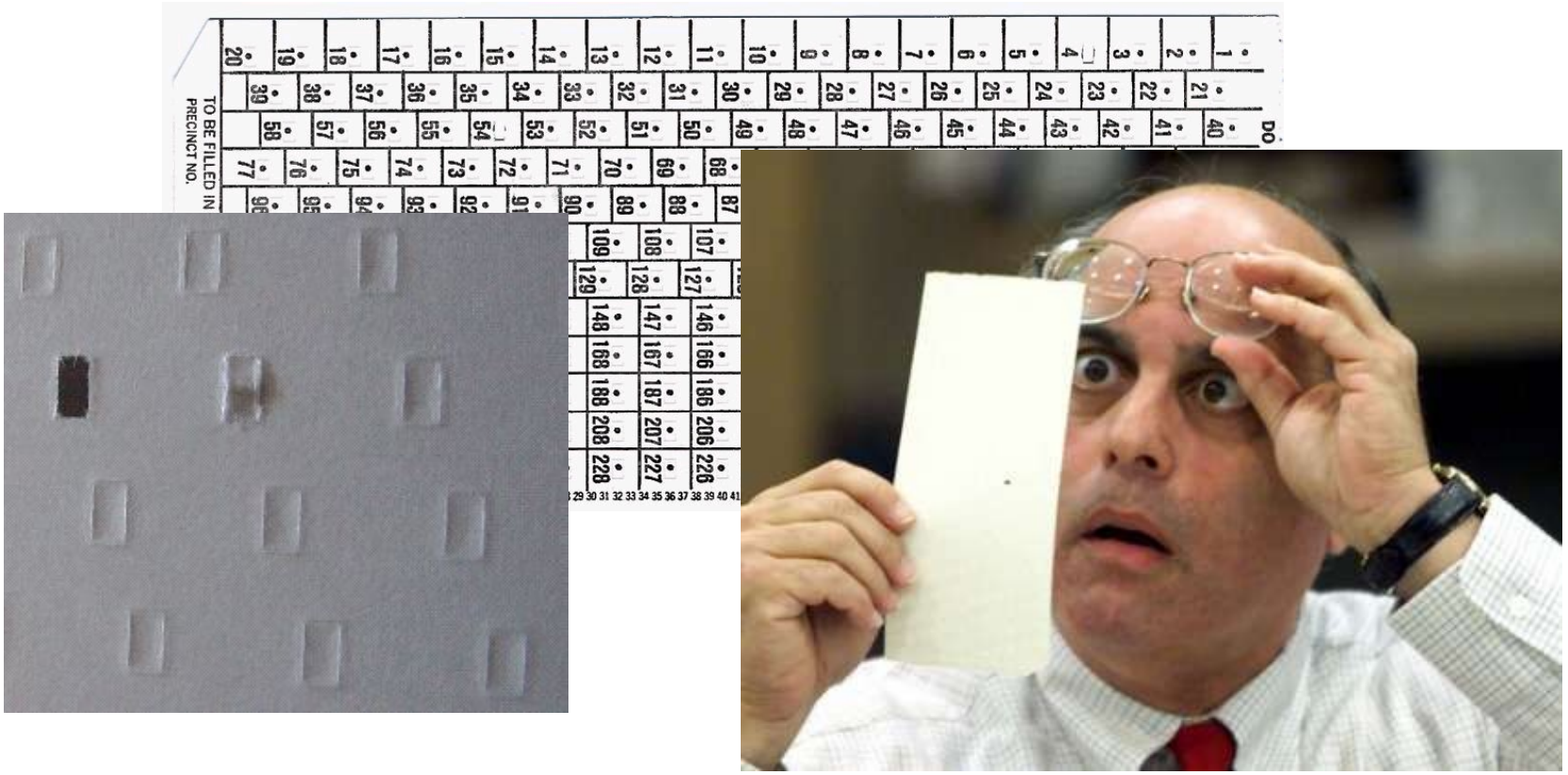
Lever Machines



- Invented in 1892
- Production ceased in 1982

Punch Card Voting

- Circa 1960, based on computerized punch card
- Now illegal (HAVA, Help America Vote Act, 2002)



Recent History of Electronic Voting

- "Prehistory"
- Year 2000 elections and aftermath
  - How evil are "hanging chad" and "pregnant chad"?
  - Help America Vote Act (HAVA 2002)
- Rush to "computerized" voting systems
  - Better accessibility and precision – good reasons!
  - "Bleeding" edge adoption risks
- Issues with technology
  - Premature deployment of immature technology
  - Potential for reducing errors / controlling interference
  - Potential for increasing errors / allowing interference

Onsite Voting (vs. Online Voting)

- We are concerned with ***onsite voting***
- Voting and tabulation will be performed locally
- This is *not* a networking problem
  - A major challenge for (online) e-voting is implementing a private channel from the ballot casting process to the tabulation process. This is not of import here.
  - *"electronic voting from home should perhaps forever remain too risky a fantasy"*

Ron Rivest

Glossary

- VT: voting terminal or voting tabulator
- CTS: central tabulation system
- EMS: election management system
- DRE: direct recording electronic (w/ paper / paperless)
- TS: touch screen
- OS: optical scan
- VVPB: voter verified paper ballot
- VVAT: voter verifiable audit trail

Modern Equipment

Touch Screen
DRE

Optical Scan

Other, e.g.,
Vote-by-phone

Optical Scan Tabulators

OFFICIAL BALLOT

CONSOLIDATED GENERAL ELECTION
SANTA BARBARA COUNTY, CALIFORNIA
NOVEMBER 5, 2002

INSTRUCTIONS TO VOTERS: To vote for the candidate of your choice, completely fill in the OVAL to the LEFT of the candidate's name. To vote for a person whose name is not on the ballot, darken the OVAL next to and write in the candidate's name on the Write-in line. To vote for a measure, darken the OVAL next to the word "Yes" or the word "No". All distinguishing marks or erasures are forbidden and make the ballot void. If you tear, deface, or wrongly mark this ballot, return it and get another. VOTE LIKE THIS: ● VOTE BOTH SIDES

STATE

GOVERNOR
Vote for One

- GARY DAVID COPELAND — Chief Executive Officer — Libertarian
- BILL SIMON — Businessman/Charity Director — Republican
- REINHOLD GULKE — Electrical Contractor/Farmer — American Independent
- GRAY DAVIS — Governor of the State of California — Democratic
- IRIS ADAM — Business Analyst — Natural Law
- PETER MIGUEL CAMEJO — Financial Investment Advisor — Green
- Write-In

LIEUTENANT GOVERNOR
Vote for One

- PAT WRIGHT — Ferret Legalization Coordinator — Libertarian
- PAUL JERRY HANNOSH — Educator/Businessman — Reform
- BRUCE MC PHERSON — California State Senator — Republican
- KALEE PRZYBYLAK — Public Relations Director — Natural Law
- CRUZ M. BUSTAMANTE — Lieutenant Governor — Democratic
- JIM KING — Real Estate Broker — American Independent
- DONNA J. WARREN — Certified Financial Manager — Green
- Write-In

INSURANCE COMMISSIONER
Vote for One

- DALE F. OGDEN — Insurance Consultant/Actuary — Libertarian
- DAVID I. SHEIDLOWER — Financial Services Executive — Green
- GARY MENDOZA — Businessman — Republican
- JOHN GARAMENDI — Rancher — Democratic
- STEVE KLEIN — Businessman — American Independent
- RAUL CALDERON, JR. — Health Researcher/Educator — Natural Law
- Write-In

MEMBER, STATE BOARD OF EQUALIZATION
2ND District
Vote for One

- TOM Y. SANTOS — Tax Consultant/Realtor — Democratic
- BILL LEONARD — State Lawmaker/Businessman — Republican
- Write-In

UNITED STATES REPRESENTATIVE

24TH District
Vote for One

- ELTON GALLEGLY — U.S. Representative — Republican

FOR ASSOCIATE JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE JUDITH M. ASHMANN be elected to the office for the term prescribed by law?
YES NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE KATHRYN DOI TODD be elected to the office for the term prescribed by law?
YES NO

FOR PRESIDING JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION THREE

Shall PRESIDING JUSTICE JOAN DEMPSEY KLEIN be elected to the office for the term prescribed by law?
YES NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL
2nd APPELLATE DISTRICT, DIVISION FOUR

Shall ASSOCIATE JUSTICE GARY HASTINGS be elected to the office for the term prescribed by law?
YES NO

First used in 1962

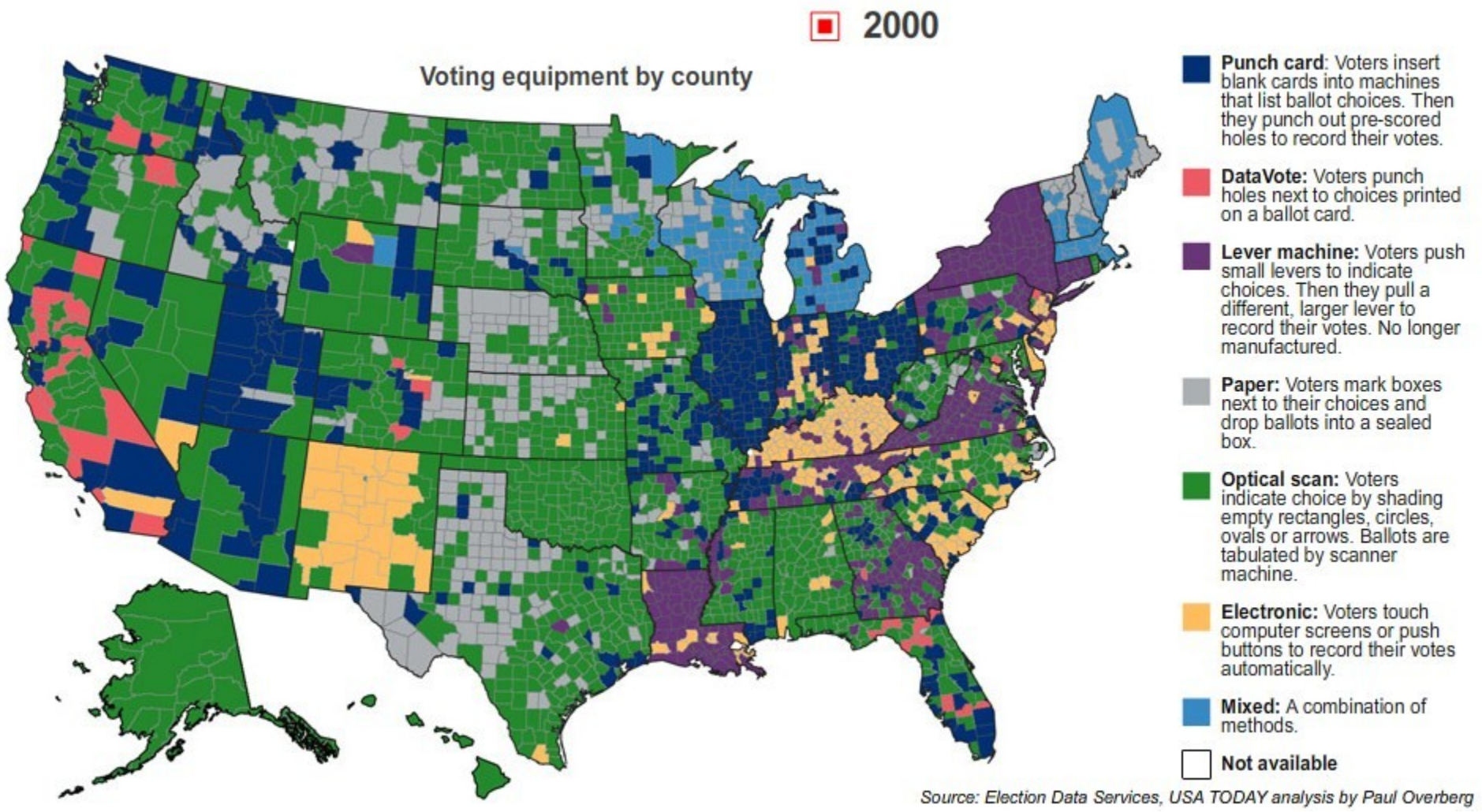
DRE / Touch Screen

- Direct Recording by Electronics
- First used in 1970's
- Essentially, a stand-alone computer

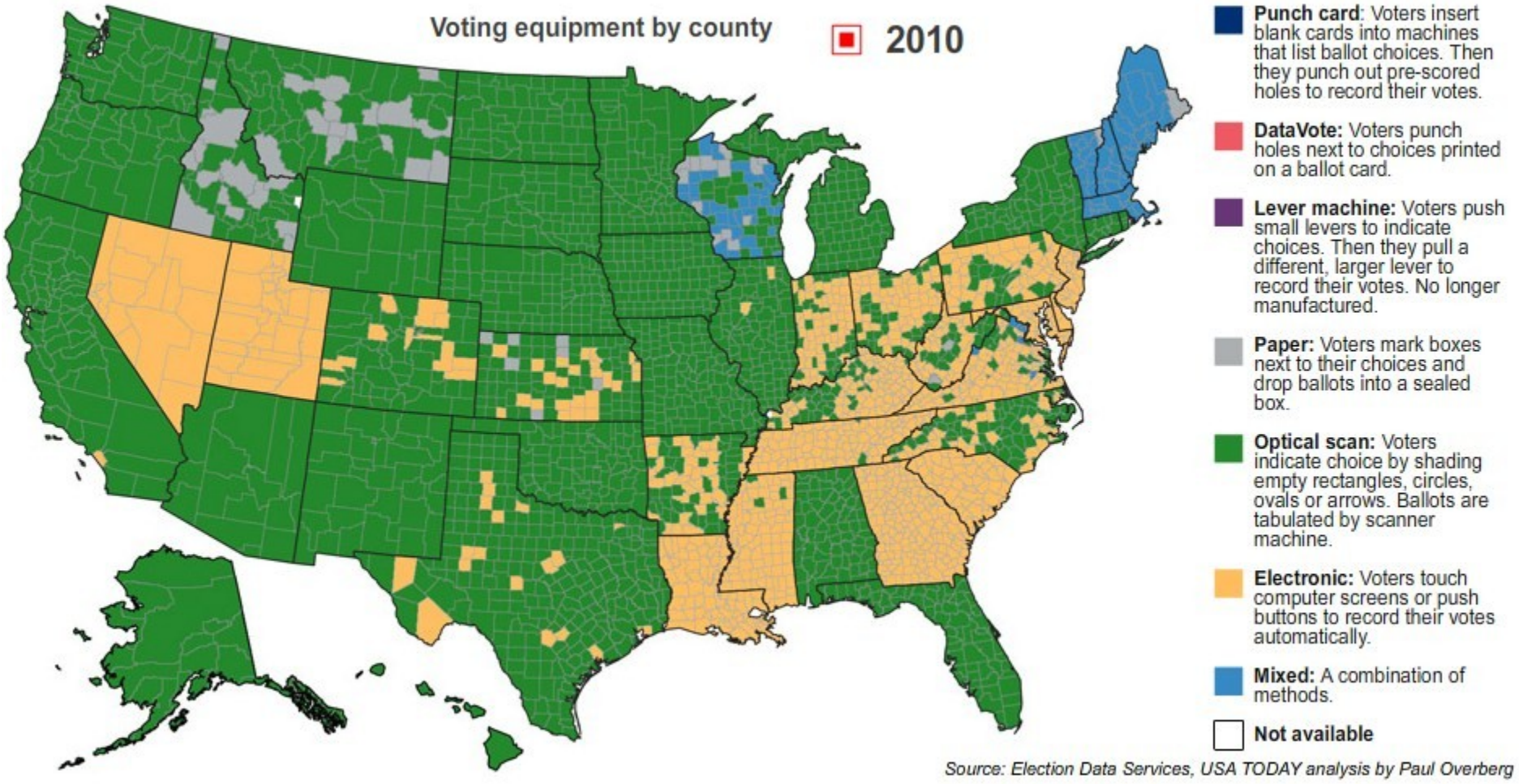
DRE + VVPAT

- DRE+Voter-Verified Paper Audit Trail.
- First used in 2003.

Voting Equipment in 2000



Voting Equipment in 2010



DRE vs. OS Issues

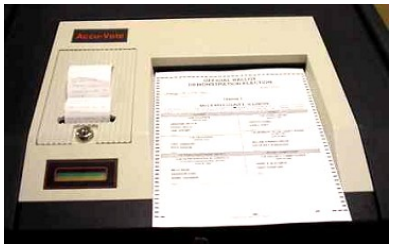
- DRE: Direct Recording, Electronic; Touch Screen
- Advantages
  - Potential for better precision
  - Potential for reducing undervotes
  - Potential for better accessibility
  - Flexible user interface
  - Can incorporate assistive technologies for disabled
  - No need to preprint ballots

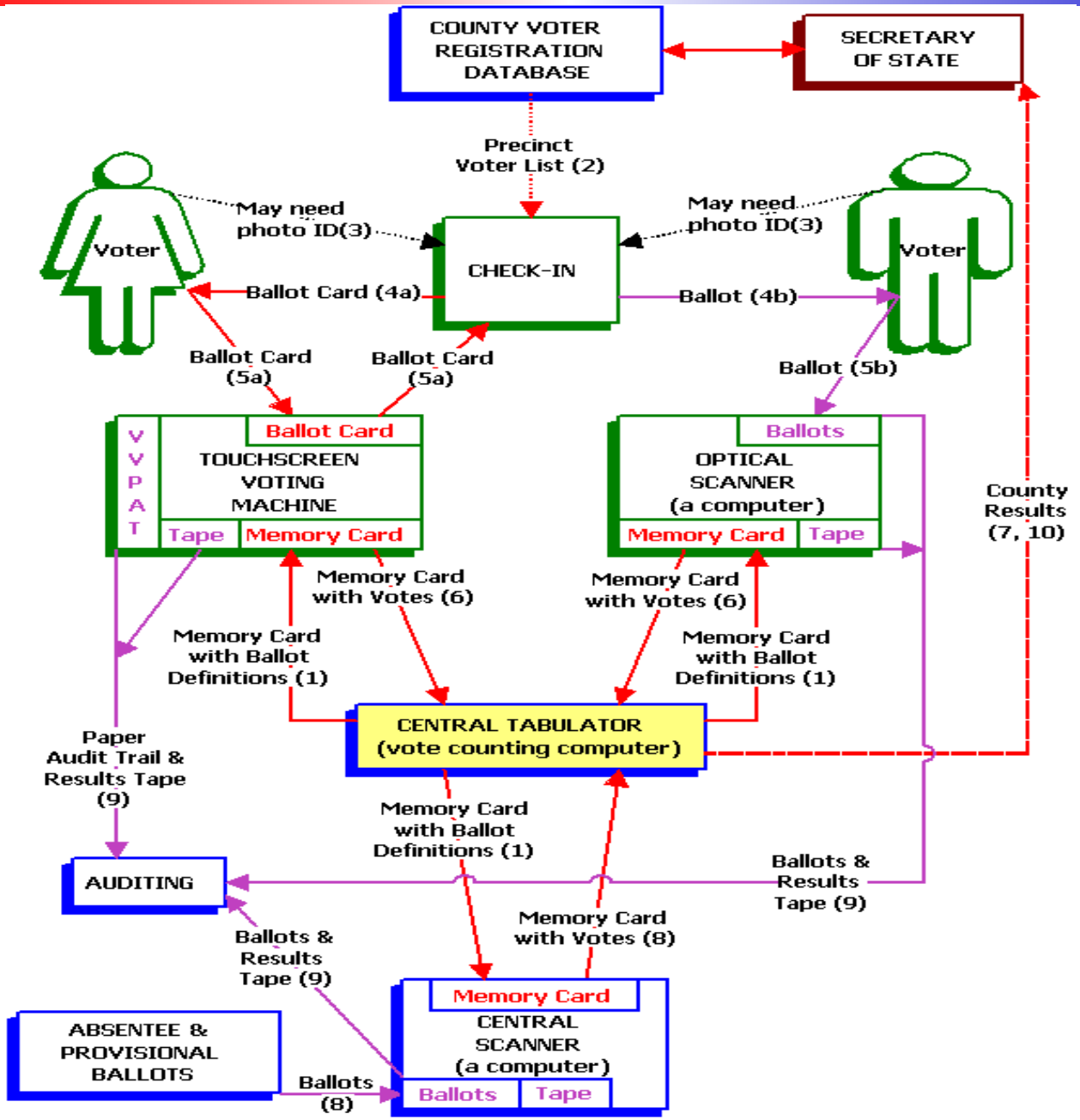
DRE vs. OS Issues

- DRE:Disadvantages
  - Paperless systems are inherently risky
    - No VVAT/VVPB
    - Malfunctions can be devastating
  - DRE-produced paper ballots
    - Better, but no direct VVPB
  - Fault tolerance issues; recovering votes
  - More complex systems: harder to avoid problems
- Premature adoption of poorly-designed machines
  - By 2009 the States will have scrapped $1B of recently purchased DREs

DRE vs. **OS** Issues

- OS: Optical Scan / voter-marked ballots
- Disadvantages
  - Less accessible
  - Potential for voter-introduced ambiguity
  - Need pre-printed ballots: quantity and precision
- Advantages
  - Serve as “tabulators”, not “voting machines”
    - Failures do not interfere with the voting process
  - Voter-Verified Audit Trail enables manual audits
  - High throughput; reduced waiting time
- Adoption on the rise: over 50% of districts




COUNTY VOTER REGISTRATION DATABASE
SECRETARY OF STATE
Precinct Voter List (2)
Voter
May need photo ID(3)
CHECK-IN
May need photo ID(3)
Voter
Ballot Card (4a)
Ballot (4b)
Ballot Card (5a)
Ballot Card (5a)
Ballot (5b)
VVPAT
Ballot Card
TOUCHSCREEN VOTING MACHINE
Tape
Memory Card
Ballots
OPTICAL SCANNER (a computer)
Memory Card
Tape
County Results (7, 10)
Memory Card with Votes (6)
Memory Card with Votes (6)
Memory Card with Ballot Definitions (1)
Memory Card with Ballot Definitions (1)
CENTRAL TABULATOR (vote counting computer)
Paper Audit Trail & Results Tape (9)
Memory Card with Ballot Definitions (1)
AUDITING
Ballots & Results Tape (9)
Ballots & Results Tape (9)
Memory Card with Votes (8)
Memory Card
CENTRAL SCANNER (a computer)
ABSENTEE & PROVISIONAL BALLOTS
Ballots (8)
Ballots
Tape

Attacker Objectives

- Modify election results
- Violate the privacy of the voter
- Disrupt the election process
- Extracting voting receipts (to sell or to coerce)
- Inaccurate audit-trail
- Bias results through interface manipulation

Discovering Vulnerabilities

- Given a Voting Terminal where to look for vulnerabilities?
- What are the critical areas that are frequently vulnerable in a computer system?

Bootstrapping Vulnerabilities

- Bootstrapping:
  - the process by which a computer system "pulls itself" out of storage and gradually comes to a fully functional state
- Boot-loader
  - The first process to be activated.
- Can the boot process be "tampered"?

Injection Vulnerabilities

- System expects input that belongs to a Language
- Parses the input and executes appropriate action
- Inputs not in the Language should be rejected
  - But they are not always rejected
  - Membership may be hard (bad design choice)
  - Even if it is easy, decision test may not be properly implemented
- Integrity checking, including cryptographic, prone to
  - Malformed input injection
  - Code injection

Authentication Vulnerabilities

- Various roles need to be identified by voting equipment
  - voter, poll-worker, administrator
- Password-based authentication?
  - dictionary attacks
- Smartcard-based authentication
  - smartcard integrity
- In general look for
  - Poor design choices

Configuration Vulnerabilities

- Obvious reset / power buttons
- Exposed/accessible hardware ports
- Sequential paper trail
- Hard to verify VVAT printing correctness
  - that only a single VVAT record is printed or
  - that spontaneous records are not printed
- Voter privacy
  - A voting terminal should never be in a state where a voter can obtain a receipt by taking a picture (harder to guarantee with DRE)

Use of Tools

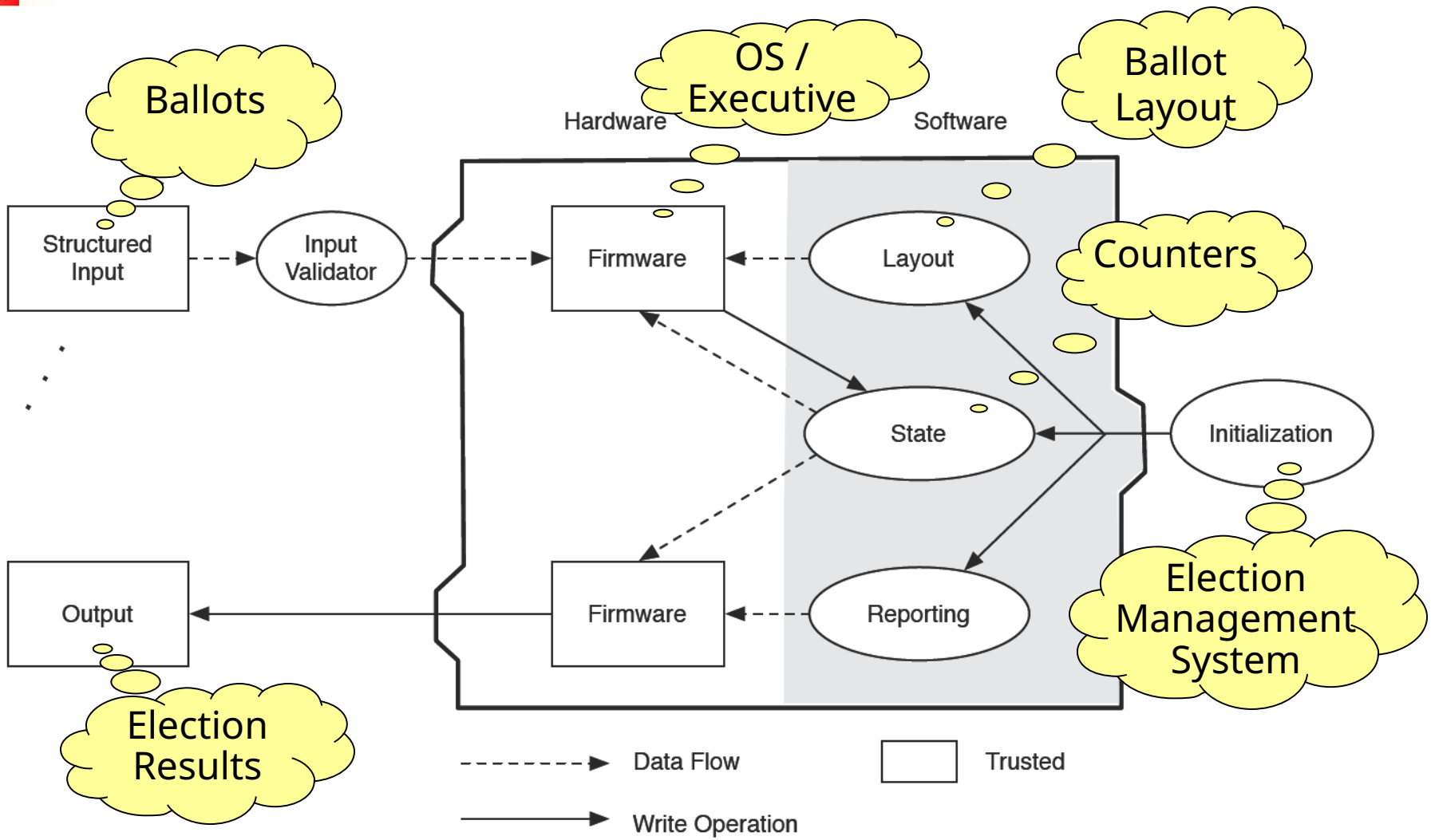
- Vulnerability associated with the use of tools
  - Using tools, such as crypto & authentication may create a false sense of security
- "Using good tools" is not the same as "good use of tools"
  - "Do not use cryptography, use a cryptographer" [A. Kiayias]
- Vulnerabilities
  - Poor use of crypto
  - Poor use of authentication
  - Poor understanding of the underlying OS

"Central Processing" Vulnerabilities

- Election Mgmt System (EMS) and/or Central Tabulation System (CTS) vulnerabilities
  - Incorrect Voting Terminal programming/ballot layout
  - Voting Terminal impersonation during post-election transfer of results to CTS
  - Vulnerabilities during results aggregation stage
  - Network transmission… let's not even touch that!

- (Also all are open to insider attacks – but this is not specific to electronic voting)

Special Purpose Trusted Computing Platform



What is inside a Voting Terminal?

- Typical computer system: processor, memory, etc.
- Storage
  - Hard disc, non-volatile memory
  - Removable storage: memory card, USB ports
- Peripherals
  - Printer
  - Communication ports, modems
- Input devices
  - Touch screen, optical scanner, keypads
- Software
  - Operating system
  - Executive, firmware, language processor, …

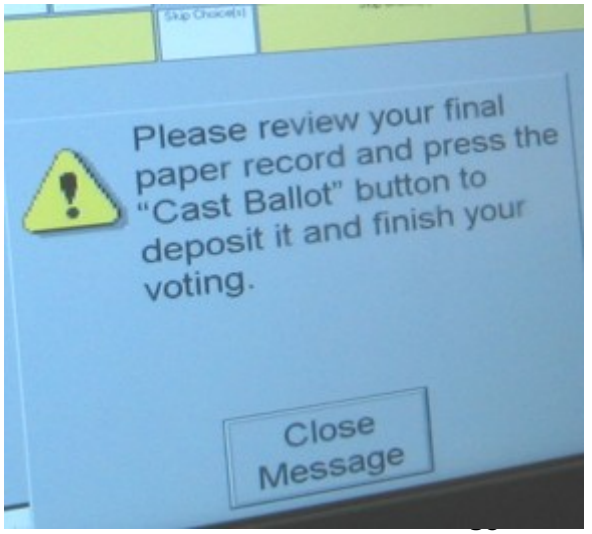
What is inside a Voting Terminal?

- What else can be found inside a voting terminal?
- Evidence of Internet access
- Email
- Erotic art
- Etc.

(Not in any voting terminal identified by name here or in use in Connecticut)

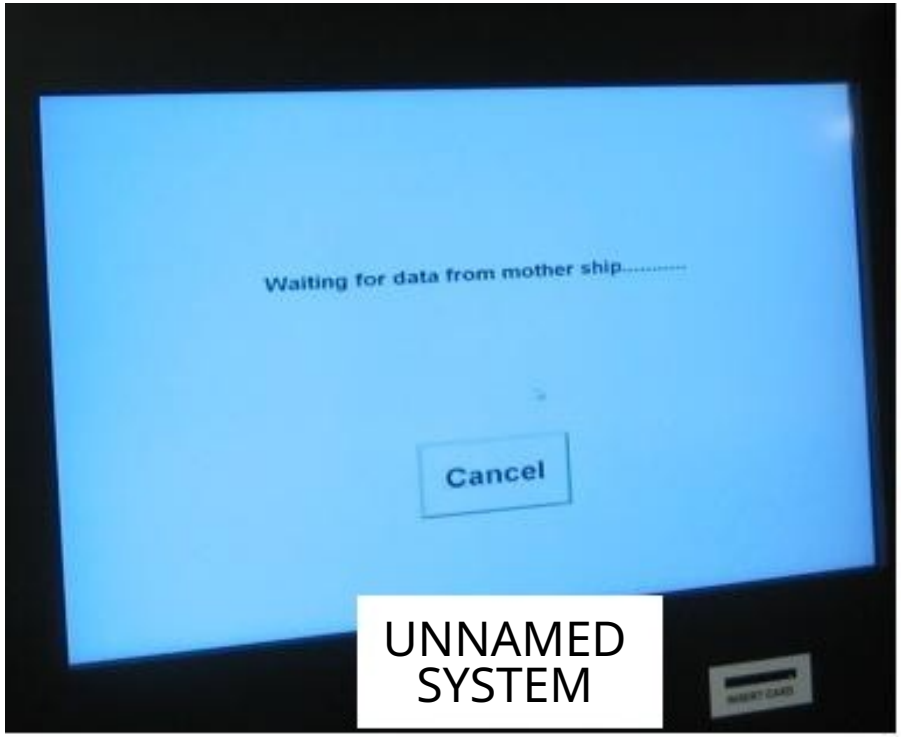
Some Troublesome Discoveries

- For the systems not identified here by name
- Hardware vulnerabilities
  - Exposed or reachable on/off switches
  - Exposed and actionable communication/USB
  - Unauthenticated software/firmware
- Operating systems vulnerabilities
  - Allow foreign code to be run
- “Benign” issues,
  - Such as voter receipts



Some Troublesome Discoveries

- For the systems not identified here by name
- The consequences
  - Compromised privacy and integrity (best case)
  - Complete control surrendered to the attacker leading to most devastating attacks…



Two Case Studies

- S. Davtyan, S. Kentros, A. Kiayias, L. Michel, N. Nicolau, A. Russell, A. See, K. Shashudhar, A. Shvartsman
  - [ACSAC 2007]
  - [EVT 2007]
  - [EVT 2008]
  - [ACM SAC 2009]
- Also see http://voter.engr.uconn.edu/voter/Reports.html

An Optical Scan Tabulator

- AccuVote Optical Scan VT
  - Manufactured by Premier (Diebold)
- Not a bleeding edge system
  - Special-purpose design
  - Small proprietary executive
- Uses voter-marked paper ballots
  - Provides voter-verified paper trail
  - Enables audits, and manual and machine recounts
- Used in most New England states
- A safe(r) choice?

AccuVote and GEMS

- AccuVote Optical Scan tabulator
  - Firmware-based executive (EPROM)
  - V25 CPU, 8088 compatible
  - Epson-Seiko 40-pin 128KB memory card
- GEMS Election Management System
  - Ballot layout: bubble geometry and counters
  - Bytecode: program to be loaded into memory card
- Memory cards
  - Inserted into AccuVote OS
  - Custom programmed and loaded from GEMS via serial line

AccuVote Optical Scan

Serial & modem ports

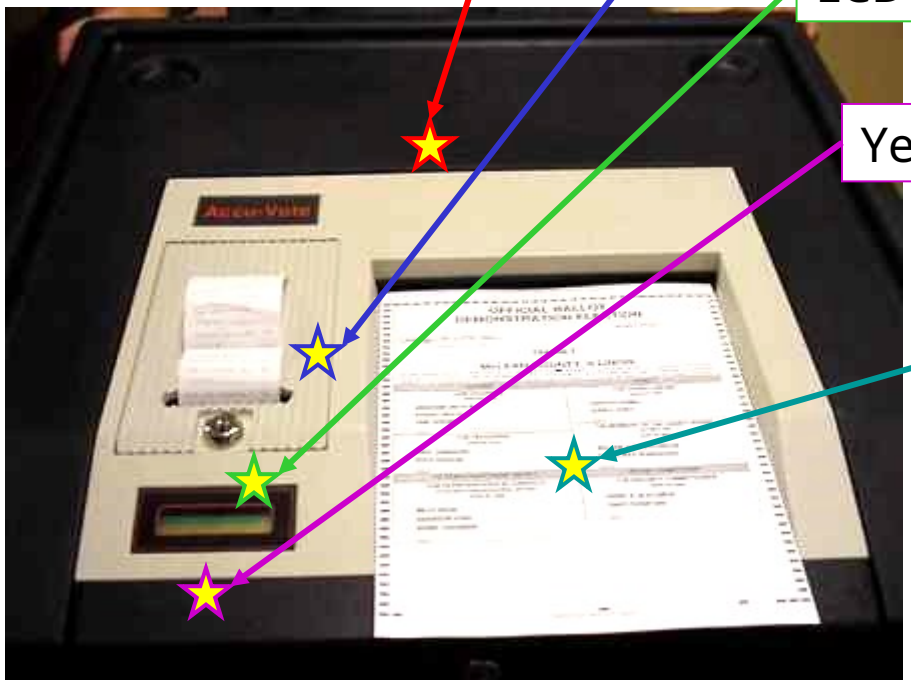
Printer

LCD display

Yes/No keys

Ballot feeder

Memory card slot



Test Report

(From Black Box Voting Archive)

wyle laboratories

Wyle Laboratories, Inc.
7800 Madison Blvd.
Huntsville, Alabama 35806
Phone (256) 837-4411 • Fax (256) 830-2109
www.wylelabs.com

REPORT NO.: 48619-09
WYLE JOB NO.: 48619
CLIENT P.O. NO.: P2003-1714
CONTRACT: N/A
TOTAL PAGES (INCLUDING COVER): 266
DATE: August 4, 2005

TEST REPORT

HARDWARE QUALIFICATION TESTING
OF THE
DIEBOLD ELECTION SYSTEMS
ACCUVOTE OPTICAL SCAN MODEL D
PRECINCT BALLOT COUNTER
(FIRMWARE RELEASE 1.96.6)

Test Report

(From Black Box Voting Archive)

FEC Req. No.	Requirement Volume 1, FECVSS 2002 Functional Requirements	Accepted	Rejected	N/A	N/T
2	Functional Capabilities				
2.2	Overall System Capabilities				
2.2.1	Security (Hardware & Software ITA)				
a.	Security accesses controls that limit or detect access to critical system components.	☑			
b.	The provided system functions that are executable only in the intended manner and order, and only under the intended conditions.	☑			
c.	The system's control logic to prevent a system function from executing, if any preconditions to the function have not been met.	☑			
d.	The safeguard that protects against tampering during system repair, or interventions in system operations, in response to system failure.	☑			
e.	The security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.	☑			
f.	Access to a system function that is restricted or controlled.	☑			
g.	Mandatory administrative procedures for effective system security.	☑			

The Hursti Attack, 2005

- Wyle Labs certifies AccuVote OS in 2005
- H. Hursti develops an attack the same year
  http://www.blackboxvoting.org/BBVreport.pdf
- Claim: memory cards can be modified so that election results are reported inaccurately/falsely

Connecticut's Response

- Connecticut Secretary of State Office establishes a relationship with UConn VoTeR Center
- One of the requests to the VoTeR Center:
  - *'Review, evaluate and report on the accuracy and findings of the report entitled "Security Alert: July 4, 2005. Critical Security Issues with Diebold Optical Scan Design" by Harri Hursti.'*
- Most States using similar technology were slow to realize (or never realized) the significance of Hursti's findings (to this day!)

Our Assessment of Threat

- The Hursti attack takes advantage of the following:
  - Memory card contains byte code and counters
  - Byte code is used for reporting functions
    - can be modified to report that the counters are 0-ed (even though they are not)
  - There is no integer overflow exception
    - 16-bit counters can be set to values like 65530
  - No (cryptographic) integrity check in the card
- The attack:

  Prior to election a properly programmed memory card is reprogrammed using a card reader/writer

Our Assessment of Threat

- In principle, anyone with access to the machine just before the election could replace the card with a tampered one
- A card reader/writer is required
  - from CropScan Inc.
    (not on the market)
  - ...security through obsolescence...

- It is possible to neutralize this attack at the poll-site
  - by running a machine audit mock election
    (this will reset the counters)

One Solution for Hursti Attack

- Strict control over memory cards
  - Seal the card
- Is this enough?
  - We performed additional research

Our Attack

- VoTeR Center performed additional analysis, finding another vulnerability
- Use the machine itself as card reader/writer
- Attack can withstand zero-ing the counters
- The infected terminal will perform an entire audit election correctly!
- Payload: swap candidates' tallies
- Method: tamper with the bubble sheet layout

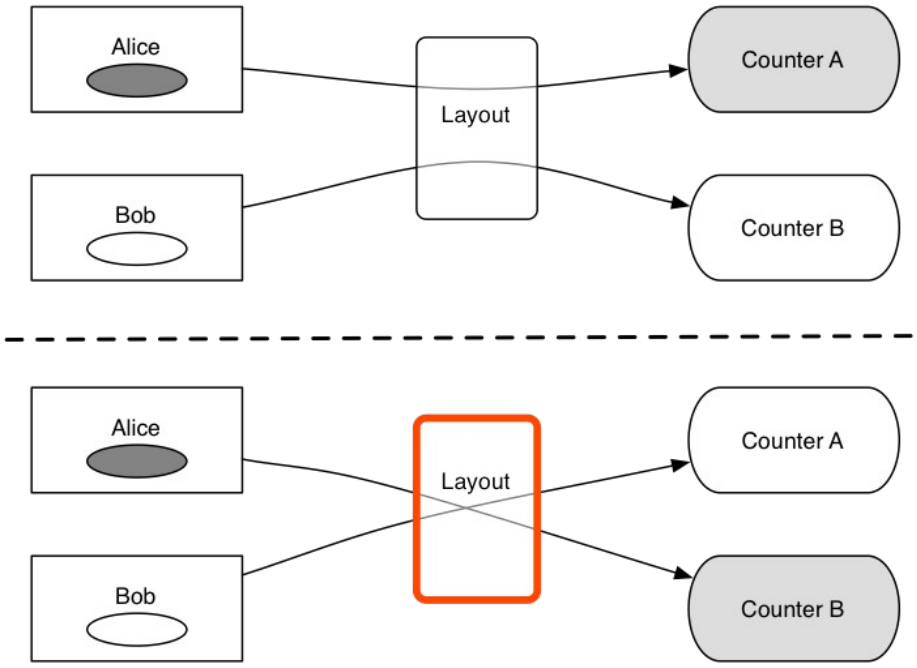
http://voter.engr.uconn.edu/voter/Reports.html

Our Attack ...

- Does **not** take advantage of a bootstrapping vulnerability
  - unlike most DRE/TS, the bootstrap process in AV-OS is at the hardware level (reflashing the firmware requires hardware tampering)
- Does **not** require any special hardware
  - no special card reader / writer
- Was **not** developed with any insider help/info
  - "Blackbox" attack
  - we never had any access to proprietary information about the terminal or vendor's design documents

Ballot Layout Attack

- Ballot Layout maps candidate name to:
  - "Bubble" location (x,y coordinates)
  - And the corresponding counter
- Stored on memory card
- Our attack swaps the votes cast for any two candidates



Delivering The Payload

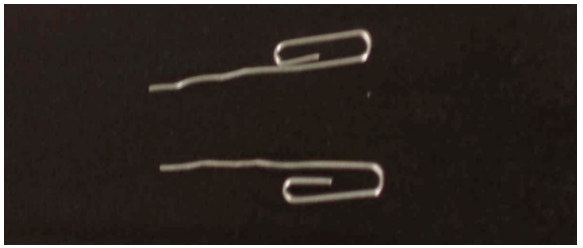
- Two Methods
  - Using Hursti attack:
    - Alter memory card directly
    - Requires memory card access
    - Requires card reader/writer
  - Our attack:
    - *Impersonate Election Management System GEMS*
    - Requires authentication

Summary of the Attack

- How our software was developed:
  - "Differential Protocol Analysis": wiretapping communication between GEMS and the tabulator
  - Reverse engineering the protocol communication
  - No access to vendor technical documents
- Our software fools the tabulator into believing it is talking to the GEMS system
- Milestones of the attack
  - Understand the byte code
  - Reverse engineering the communication integrity check
  - Recovering the PIN
  - Mapping the card contents and identifying key regions

Accessing the back side of the machine

+



=

The setup of our attack:

Use the "Diagnostic Mode"

1. "turn on the machine while depressing the yes/no buttons"
2. dump memory card contents.

Recover PIN Number

- 4-digit PIN number stored on card
- Encoding PIN+K
- Can be read using HEX editor (if you know where to look)
- K depends on machine / card number

Use “Supervisor Functions”

- Supervisor Functions include:
  - Disable printer
  - Edit communication parameters
  - Erase memory card.

Use "Supervisor Functions"

- Supervisor Functions include:
  - Disable printer
  - Edit communication parameters
  - Erase memory card
  - Program memory card by direct mode?

Burning the card

The Time Bomb

- Can get caught!
  - by an auditing mock election
- Can avoid getting caught:
  as a part of our payload we program the reporting function to be time-sensitive

Bytecode

```
F "abAgPa'USMA 1.2'ObbOccBhLA
F "'a=NeWeSaaabb'5'a$Pb'TS'Pc
F "LLAiOfNdRdI&=NeWeRdQfb' 'a
F "Rdbb' 'a>NdRda$PdWeRdc99 l
...
F "*'))E&QeNdSch$PdSchBiLXbWi
F "$XbSecLE=NeSed''aXb('RACE
F " PARTY:'%bddSed)LEQhXb('#
F " TO VOTE FOR '%bfkYSef)Xb'
F "Sema)GXb''LOi+*+SeoaSenaSe
F ")E>SegaBzLE=NeSek'Y'aXb('#
F "b'Write In Candidates'Xb'E
F "b)LLLLXbWfy'*'LAzOxaOyaHfE
F "Qx9999 Xb(%avvSfc%bddRd)Xb
F "aooSfc%acc''%aeeRd%bekYQx)
F "dGPd''LE<Sfe65535 Oy+QySffaLGE=NeSee'X'aE<Sfe65535 PdSbgSfdF>"
F "SfdbPdSbg-SfdbGPd''LF<Sfe65535 PdSbgSfdGPd''LE<Sfe65535 Oy+Qy"
F "SffaLLE>Sffa9999 Xb(%avvSfc%bddRd)Xb(' '%bf"
F "kYSffa)F=NeRd''aXb(%auuSfc%bekYSffa)GXb(%aooSfc%acc''%aeeRd%b"
F "ekYSffa)LLL AsXb'WE, THE UNDERSIGNED,'Xb'DO HEREBY CERTIFY THE"
F "'Xb'ELECTION WAS CONDUCTED'Xb'IN ACCORDANCE WITH THE'Xb('LAWS"
F " OF THE ''STATE''.')Xb''Xb''Xb'**** SIGNATURES *'Xb''XbWf"
F "i(Wfy'.''
\n\n')XbWfk'\n'L"
```

- Untampered Bytecode

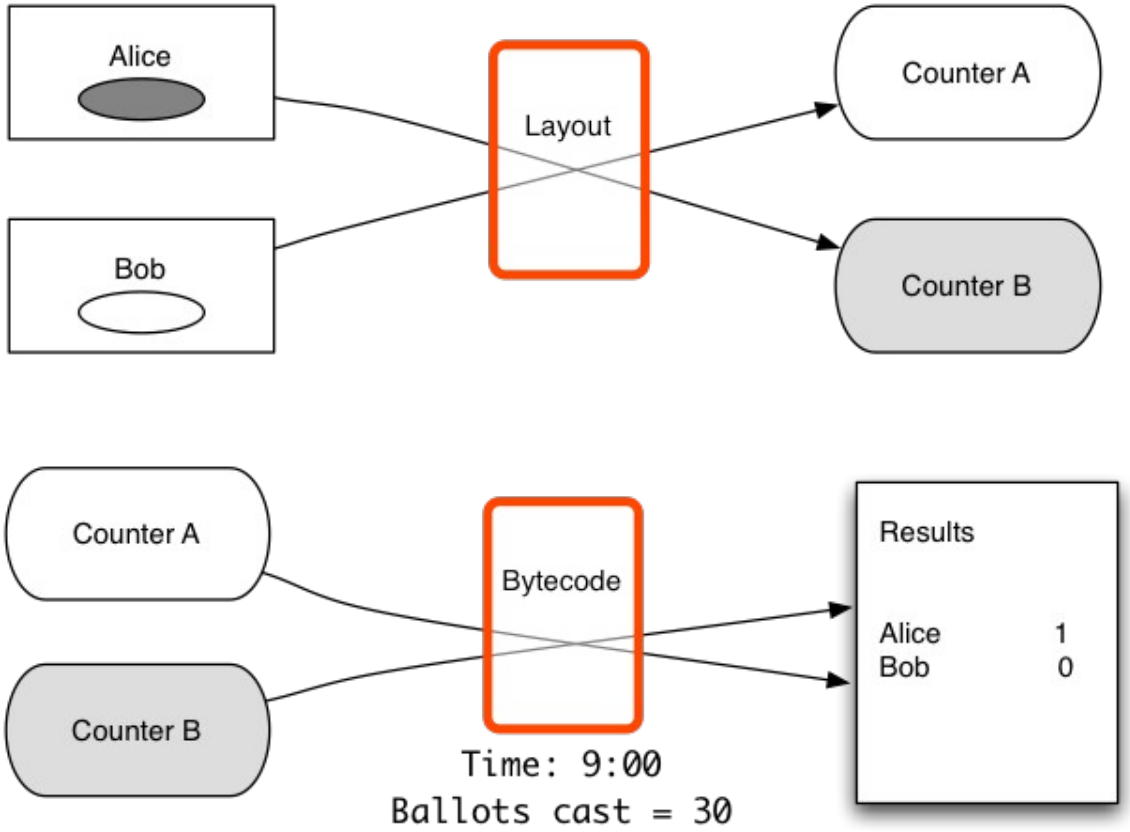
```
1 PROC z
2   %c = 0
3 FOREACH candidate
4   %c = candidate.ctr[0]
5 {Print Vote Count As %c}
6 ENDFOREACH
7 ENDPROC
```

- Tampered Bytecode

```
5 FOREACH candidate
6 IF STRCMP(candidate.name,"A")=0
7   %i = candidate.ctr[0]
8 ELIF STRCMP(candidate.name,"B")=0
9   %j = candidate.ctr[0]
10 ENDIF
11 ENDFOREACH

14 IF STRCMP(DATE,"11/07/06")!=0
15 OR STRCMP(TIME,"07:00:00")<=0
16 IF STRCMP(candidate.name,"A")=0
17   %c = %j
18 ELIF STRCMP(candidate.name,"B")=0
19   %c = %i
20 ENDIF
21 ENDIF
```

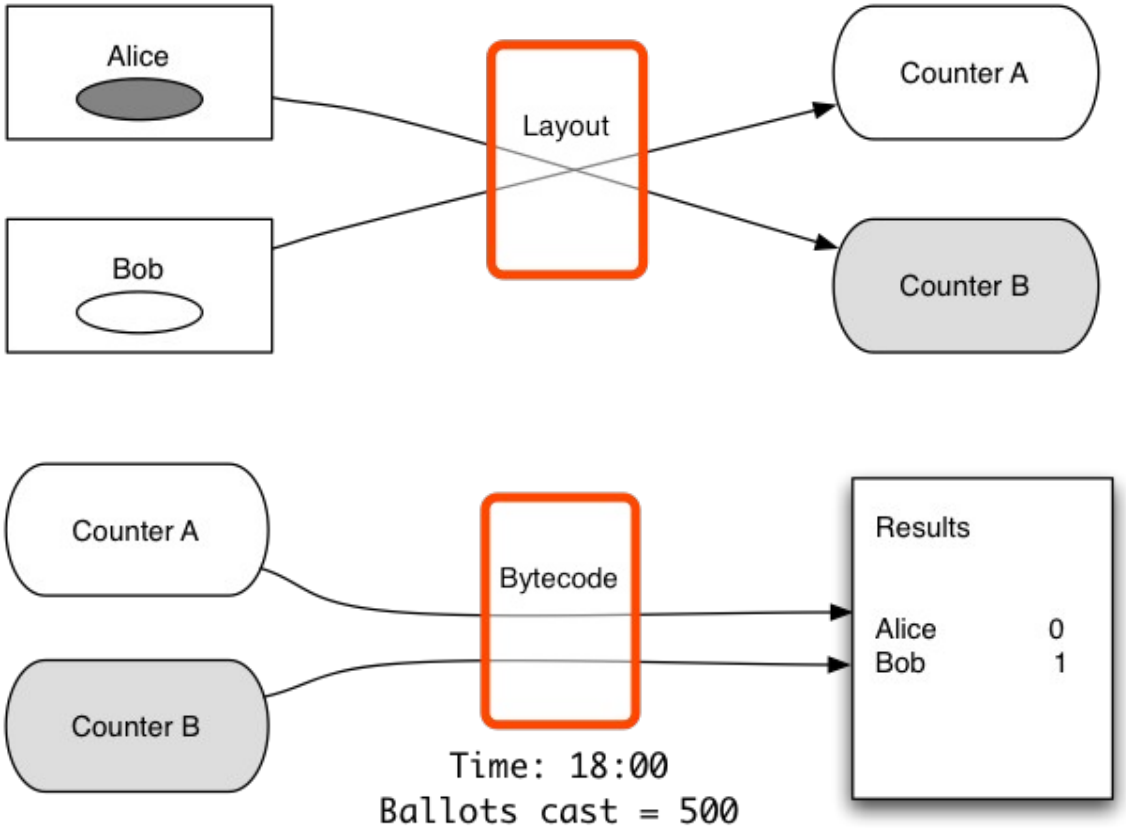
Concealing the Corruption

- Pre-Election Testing
- Votes are "un-swapped" on audit tape



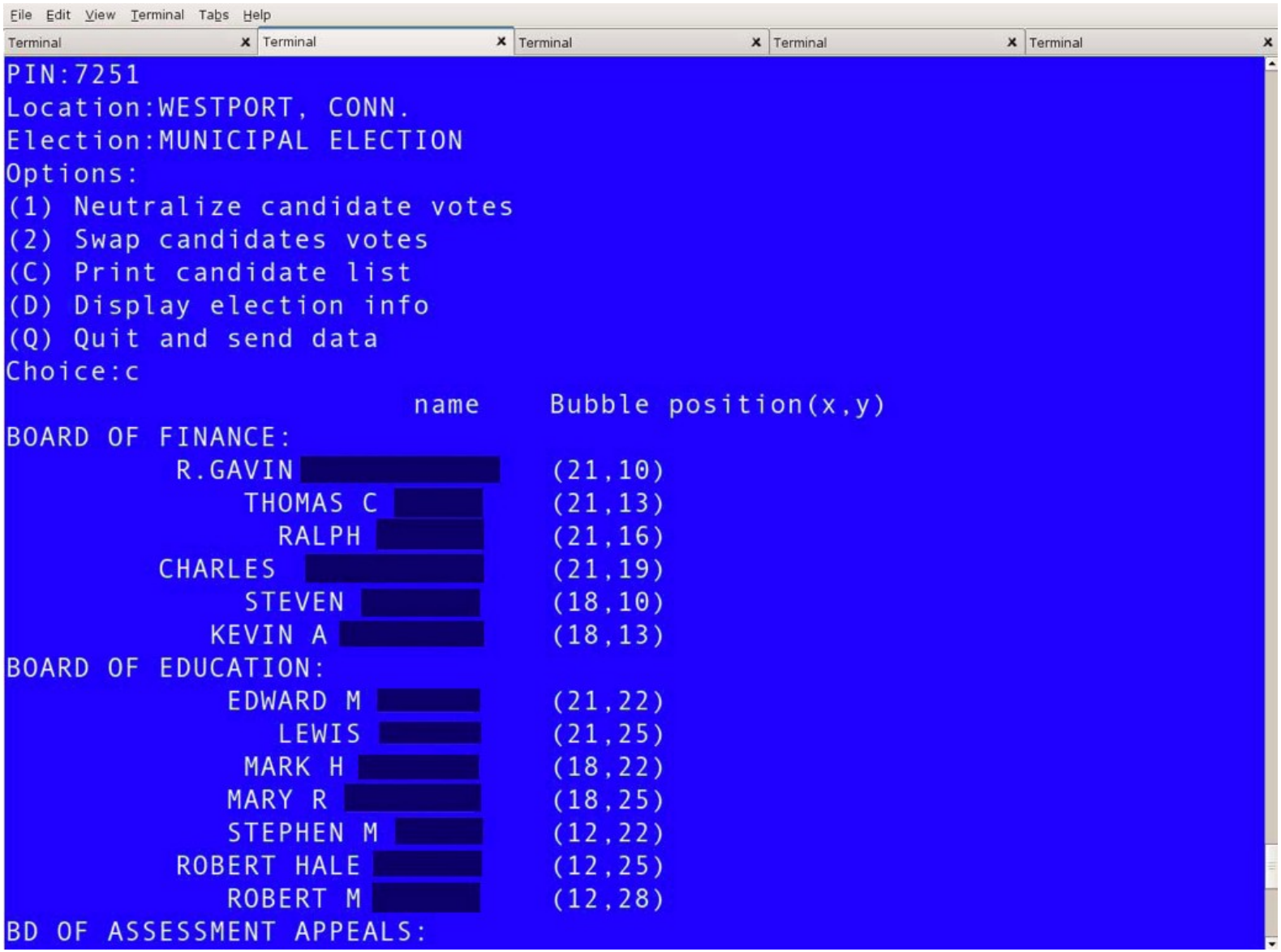
Concealing the Corruption

- During and after election
- Swapped votes are reported
- Electronic reporting also is swapped



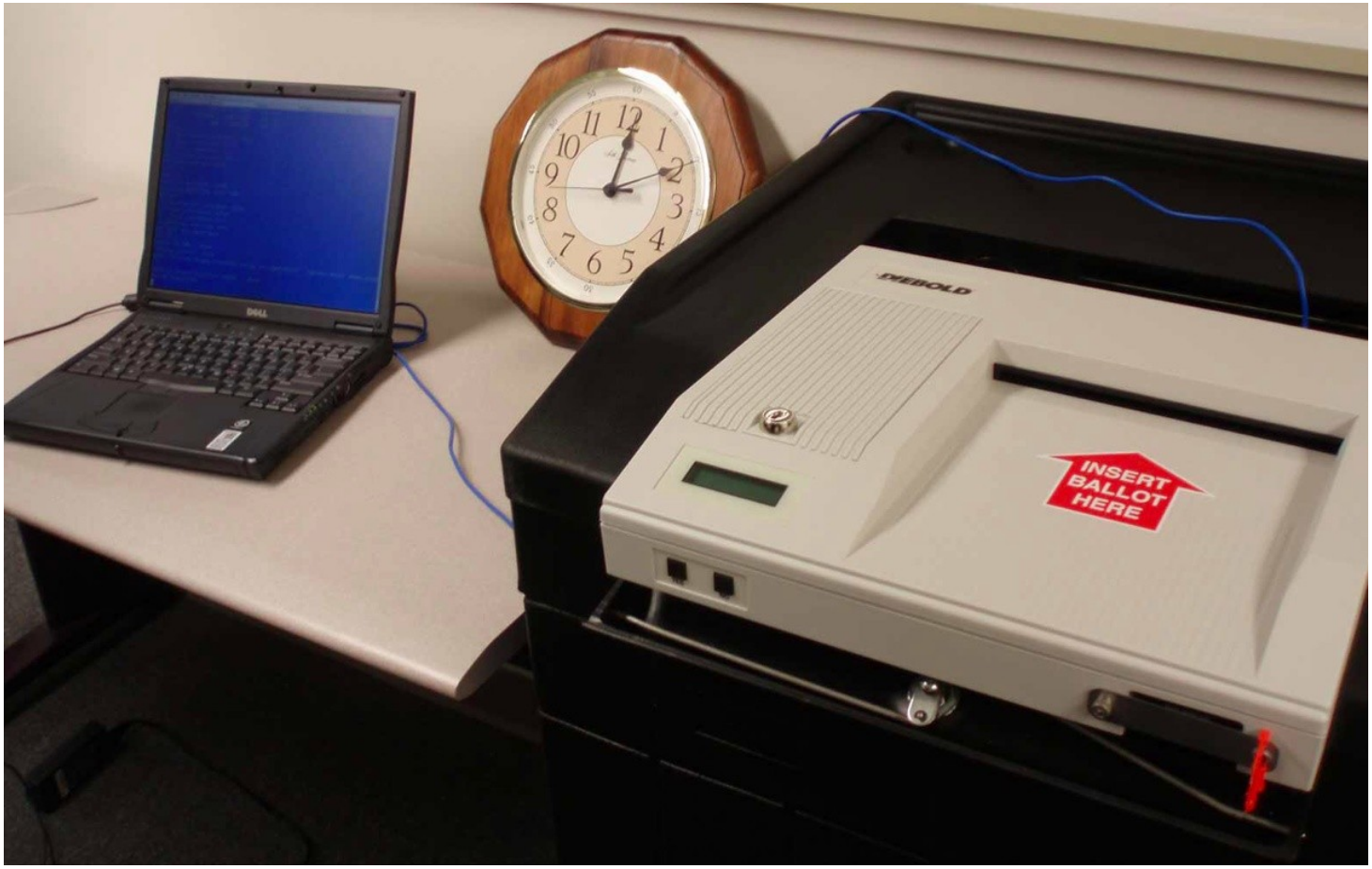
Of course all is done in our software

```
Which device to use?:/dev/ttyS1
Ready to read card from /dev/ttyS1 ...
Reading card data...Done
Parsing card data
PIN:7251
Location:WESTPORT, CONN.
Election:MUNICIPAL ELECTION
Options:
(1) Neutralize candidate votes
(2) Swap candidates votes
(C) Print candidate list
(D) Display election info
(Q) Quit and send data
Choice:
```


File Edit View Terminal Tabs Help
Terminal
Terminal
Terminal
Terminal
Terminal
PIN:7251
Location:WESTPORT, CONN.
Election:MUNICIPAL ELECTION
Options:
(1) Neutralize candidate votes
(2) Swap candidates votes
(C) Print candidate list
(D) Display election info
(Q) Quit and send data
Choice:c
name Bubble position(x,y)
BOARD OF FINANCE:
R.GAVIN (21,10)
THOMAS C (21,13)
RALPH (21,16)
CHARLES (21,19)
STEVEN (18,10)
KEVIN A (18,13)
BOARD OF EDUCATION:
EDWARD M (21,22)
LEWIS (21,25)
MARK H (18,22)
MARY R (18,25)
STEPHEN M (12,22)
ROBERT HALE (12,25)
ROBERT M (12,28)
BD OF ASSESSMENT APPEALS:

It only takes a few minutes

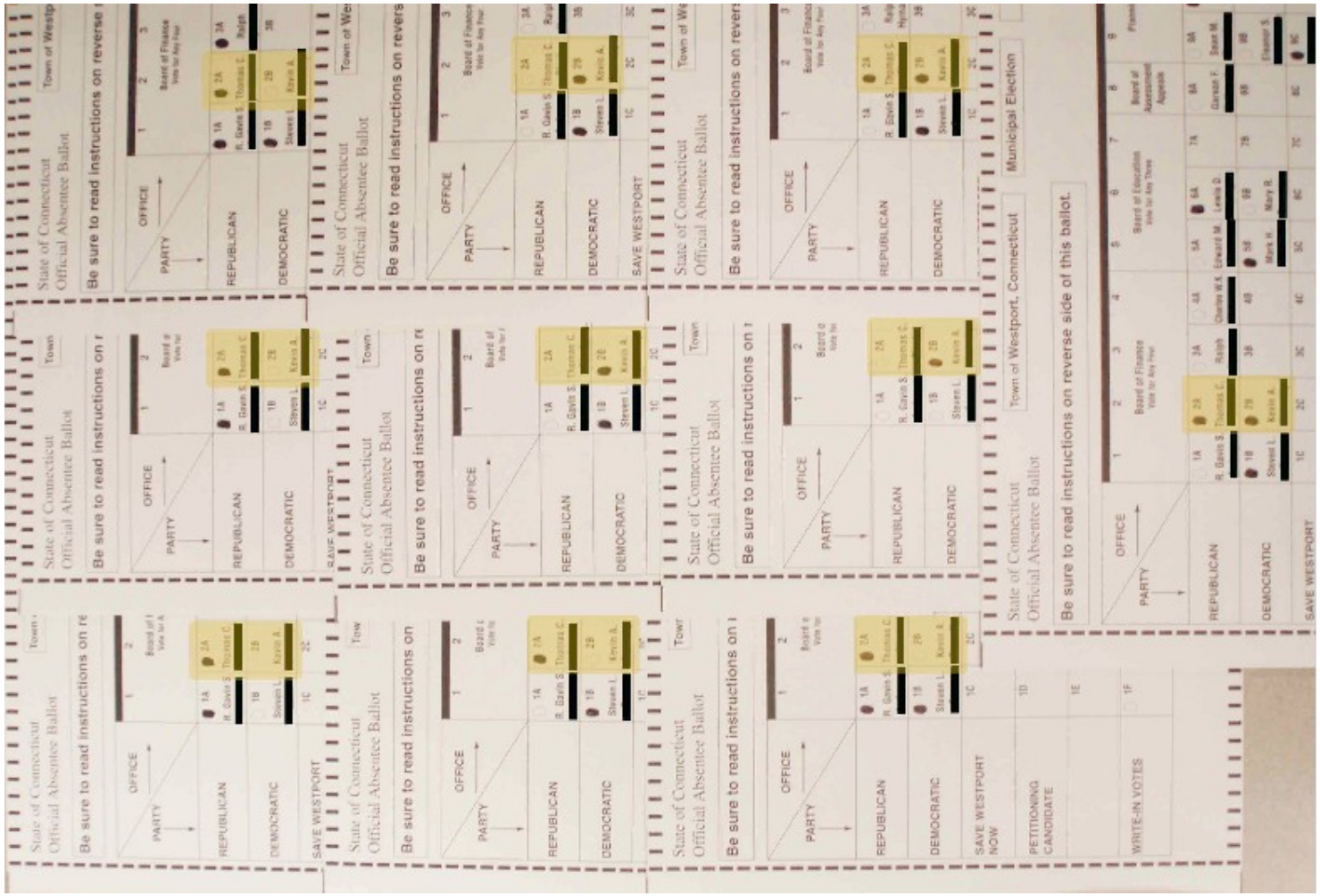
- Started at 12:02, done by 12:10, including photography

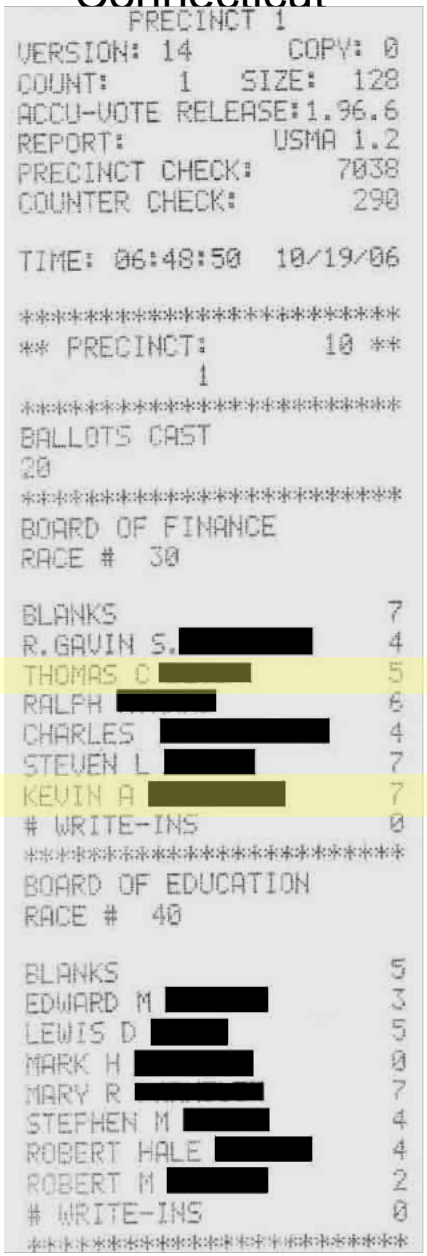


Example Election

Thomas C. = 7 votes

Kevin A. = 5 votes

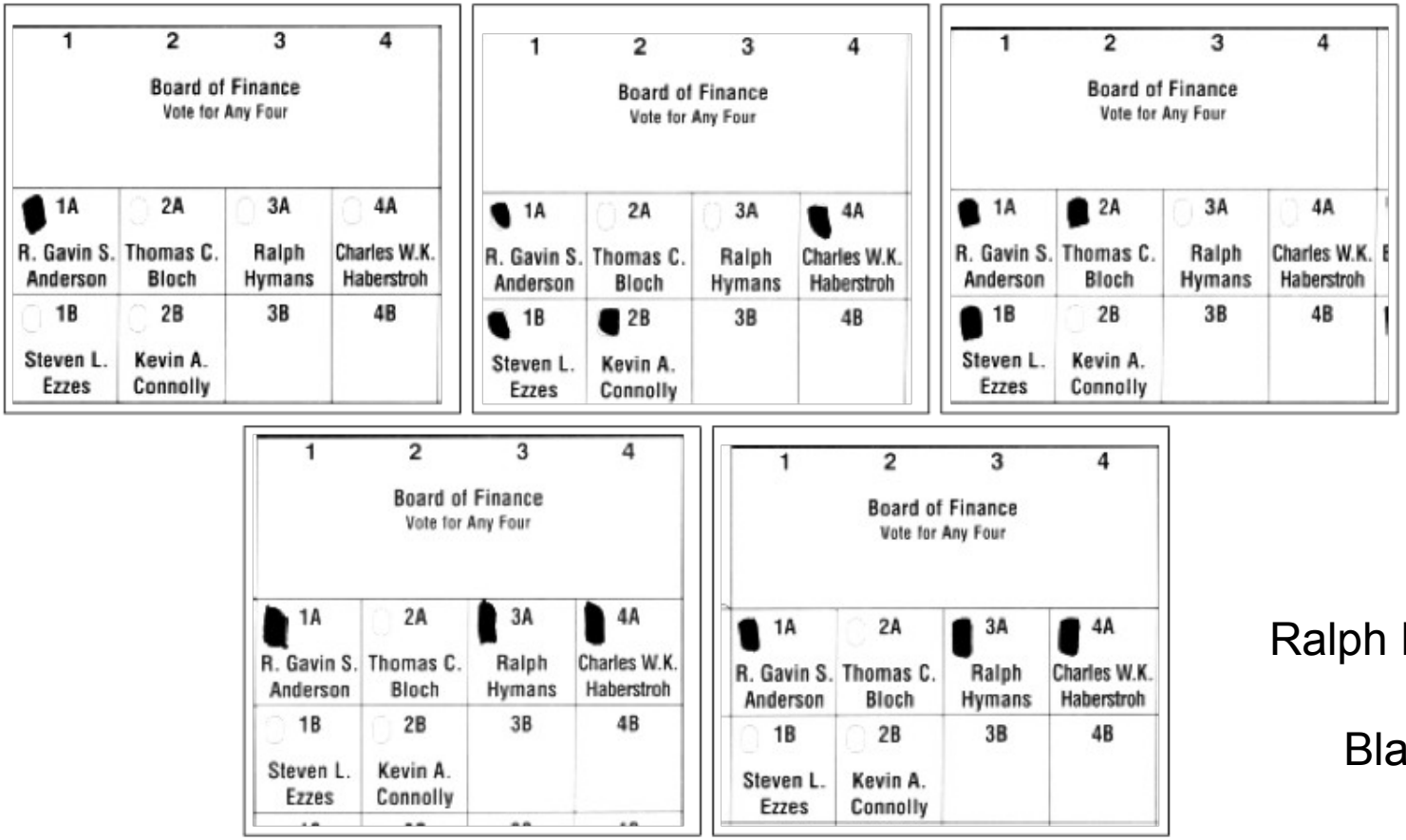




```
        PRECINCT 1
VERSION: 14        COPY: 0
COUNT:     1   SIZE:  128
ACCU-VOTE RELEASE:1.96.6
REPORT:          USMA 1.2
PRECINCT CHECK:      7038
COUNTER CHECK:        290

TIME: 06:48:50  10/19/06

************************
** PRECINCT:        10 **
             1
************************
BALLOTS CAST
20
************************
BOARD OF FINANCE
RACE #  30

BLANKS                  7
R.GAVIN S.              4
THOMAS C                5
RALPH                   6
CHARLES                 4
STEVEN L                7
KEVIN A                 7
# WRITE-INS             0
************************
BOARD OF EDUCATION
RACE #  40

BLANKS                  5
EDWARD M                3
LEWIS D                 5
MARK H                  0
MARY R                  7
STEPHEN M               4
ROBERT HALE             4
ROBERT M                2
# WRITE-INS             0
************************
```

The reported results

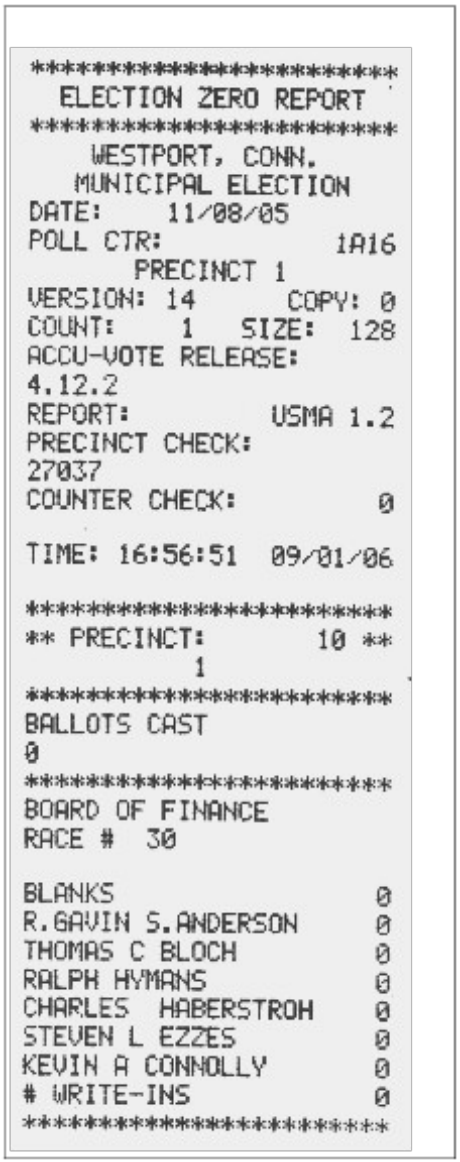
Another Nice Trick: Reassign Blanks



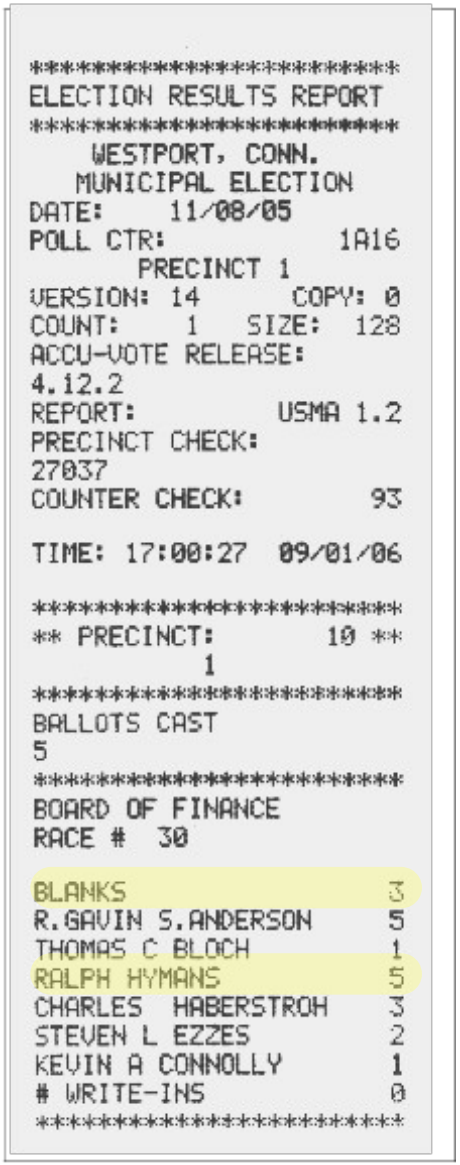
Ralph H. = 2 votes

Blanks. = 6

Election Report



```
**************************
  ELECTION ZERO REPORT
**************************
    WESTPORT, CONN.
   MUNICIPAL ELECTION
DATE:     11/08/05
POLL CTR:            1A16
       PRECINCT 1
VERSION: 14       COPY: 0
COUNT:     1   SIZE:  128
ACCU-VOTE RELEASE:
4.12.2
REPORT:          USMA 1.2
PRECINCT CHECK:
27037
COUNTER CHECK:          0

TIME: 16:56:51  09/01/06

**************************
** PRECINCT:        10 **
            1
**************************
BALLOTS CAST
0
**************************
BOARD OF FINANCE
RACE #  30

BLANKS                  0
R.GAVIN S.ANDERSON      0
THOMAS C BLOCH          0
RALPH HYMANS            0
CHARLES  HABERSTROH     0
STEVEN L EZZES          0
KEVIN A CONNOLLY        0
# WRITE-INS            0
**************************
```



```
**************************
ELECTION RESULTS REPORT
**************************
    WESTPORT, CONN.
   MUNICIPAL ELECTION
DATE:     11/08/05
POLL CTR:            1A16
       PRECINCT 1
VERSION: 14       COPY: 0
COUNT:     1   SIZE:  128
ACCU-VOTE RELEASE:
4.12.2
REPORT:          USMA 1.2
PRECINCT CHECK:
27037
COUNTER CHECK:         93

TIME: 17:00:27  09/01/06

**************************
** PRECINCT:        10 **
            1
**************************
BALLOTS CAST
5
**************************
BOARD OF FINANCE
RACE #  30

BLANKS                  3
R.GAVIN S.ANDERSON      5
THOMAS C BLOCH          1
RALPH HYMANS            5
CHARLES  HABERSTROH     3
STEVEN L EZZES          2
KEVIN A CONNOLLY        1
# WRITE-INS            0
**************************
```

Shift blanks to candidates of interest

Our Recommendations

- Our report to the State recommends
  - Strict chain-of-custody for memory cards
  - Strict chain-of-custody tabulators
  - Tamper-evident proofing of the serial ports
  - Post-election audits
- All recommendations were accepted for implementation in Connecticut for the very first election following the report, November 2006

Reactions

Connecticut News from The Hartford Courant ::: State, National, & World News On courant.com

Case Study Two

- Perhaps a more modern system is better designed?
- Consider DRE from ES&S (Premier (Diebold))
- Early-production version of the TS machine (allegedly bootlegged)
  - Security Analysis of the Diebold AccuVote-TS Voting Machine, A.J. Feldman, J.A. Halderman, E.W. Felten, September 13, 2006 http://citp.princeton.edu/pub/ts06full.pdf
- So we turn our attention to the late production TSX version, delivered by the vendor to the State of Connecticut for evaluation

The TSX machine

Uses cryptographic integrity checking for the card contents!

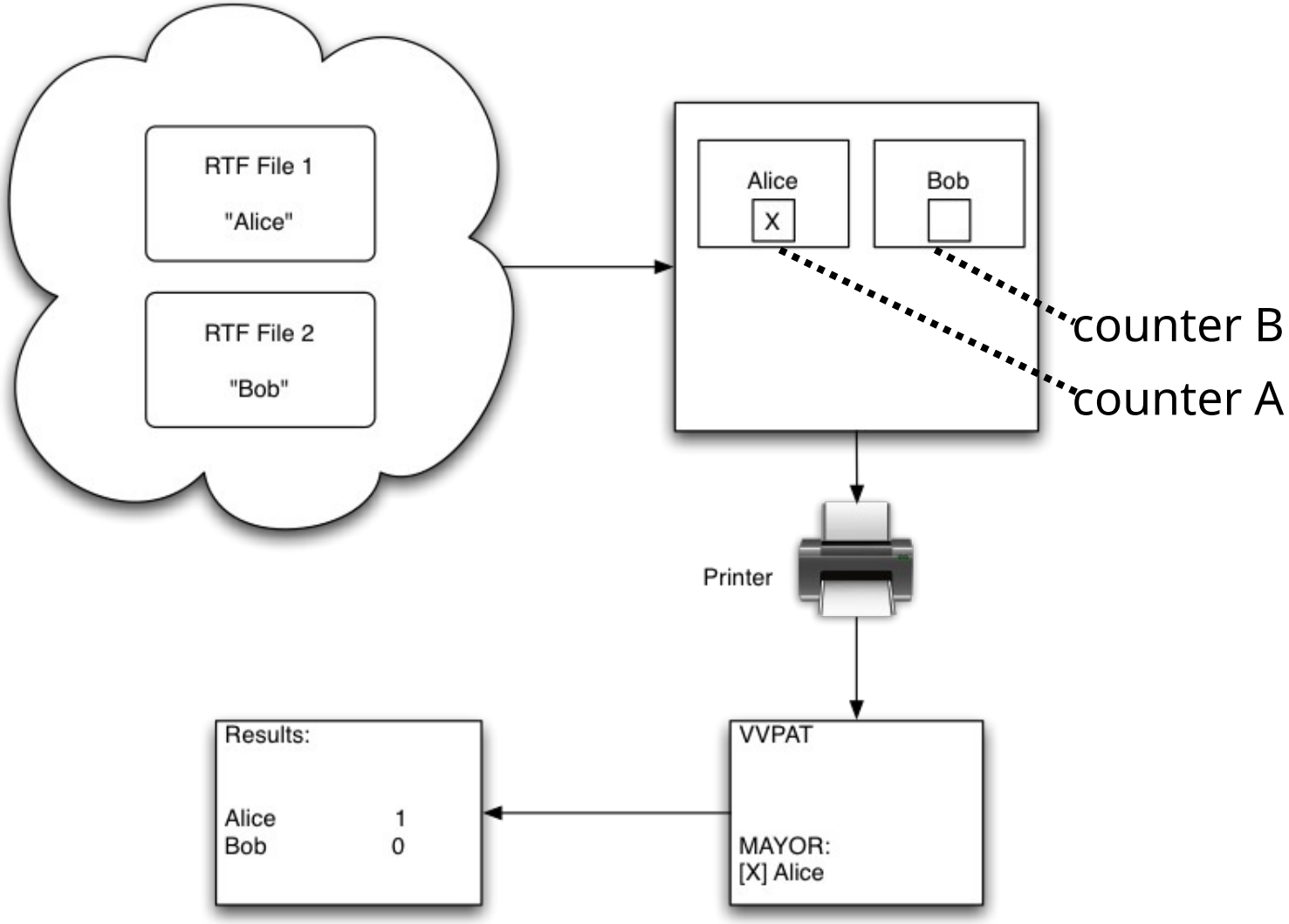
Note:
This is the real thing!
Not an obsolete version from unknown sources

Our Attack

- Circumvent cryptographic integrity checks
- Without touching the terminal itself but only the cryptographically protected card!
- Payload : *swap candidates' tallies*

http://voter.engr.uconn.edu/voter/Reports.html

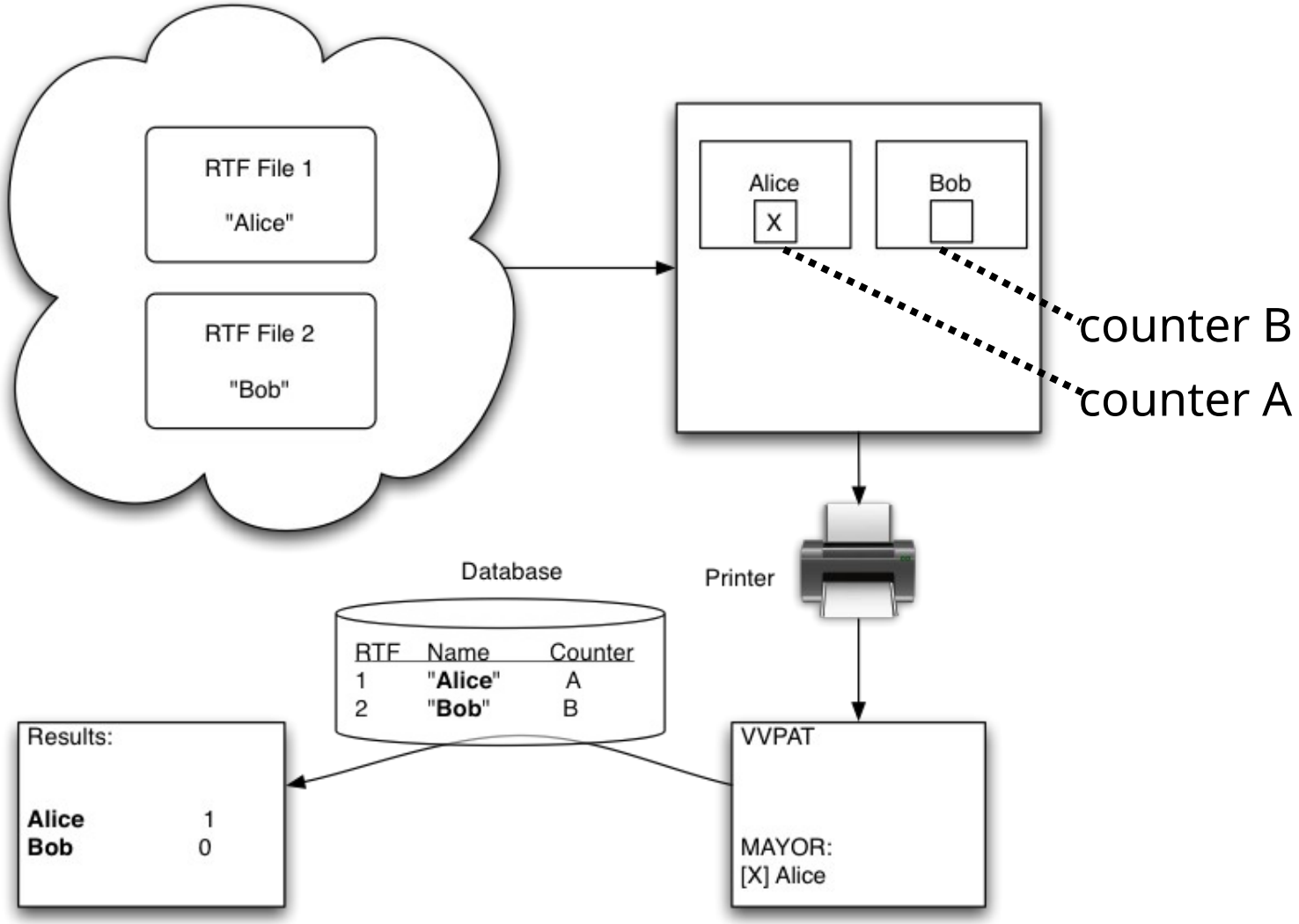
Expected Behavior



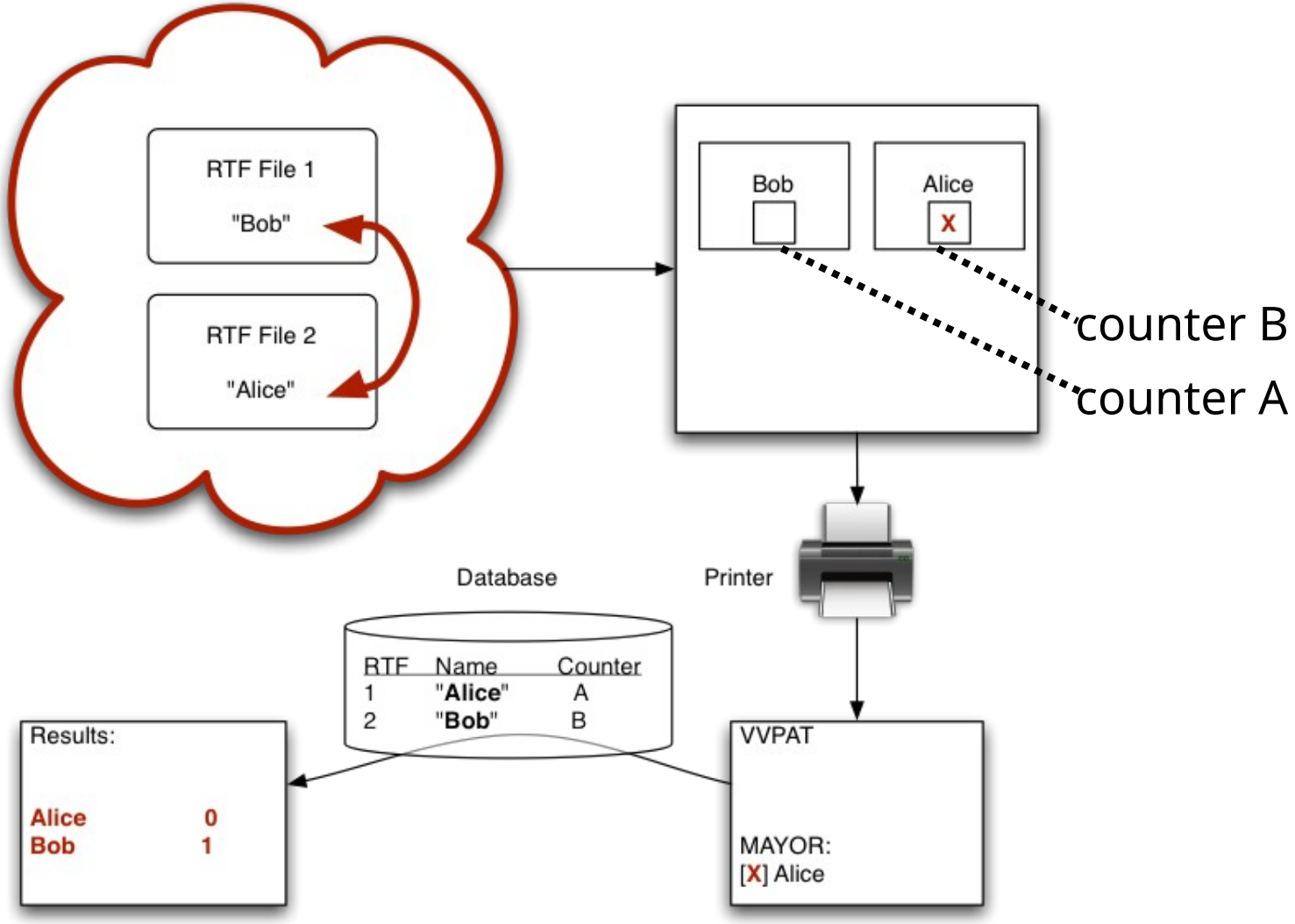
Findings

- Database of ballot layout appears signed
- Files defining slate presentation (RTF files) appear signed
- RTF files stored in something like a disk image file … not signed!
- It appears database points directly to disk image offsets

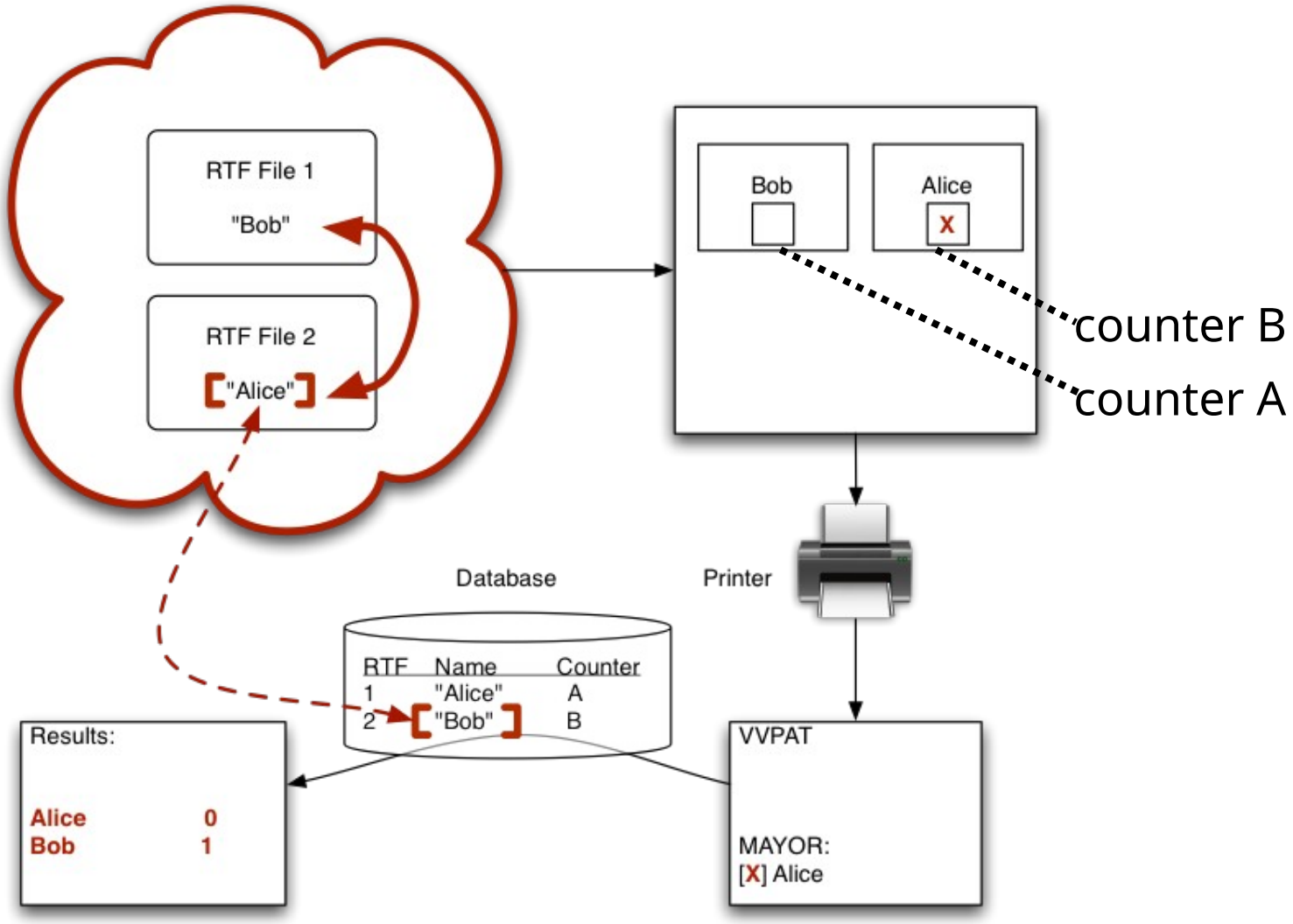
Intended TSX Behavior



Tampering with TSX



Tampering with TSX



National Landscape

- For good reasons Touch Screen DRE machines are being phased out in many States
  - Estimated $1B of equipment scrapped
- Optical Scan machines today are a safer and more secure alternative
  - VVPT and auditability
  - Connecticut's current election system
  - Many other States are now moving in this direction
- Another severe security risk: central tabulation
  - Multiple attacks are possible
  - Central tabulation is **not** used Connecticut

So What Now? What's Next?

- Longer term
  - Research and advanced development
  - Better-designed, better-engineered voting machines
  - End-to-end processes, e.g., [Ron Rivest]
  - …
- Given that the change will take some time, is there something we can do to help safeguard the (technical) integrity of the elections, other than being Luddites or Nay-Sayers

A Nagging Question

- In a Certain State it was observed that
  - Bob won most hand-counted districts, while
  - Alice carried most machine-counted districts.
  - There were good demographic reasons for this.
  - Yet… Did the machines count accurately?
  - State Officials were unable to answer the question.
- Technologists should be able to work with state governments and answer such questions.
- In Connecticut we do!

Technological and Election Audits

- Memory card audit
  - Questions:
    - Are cards properly programmed?
    - How do we know cards were not tampered with?
  - Pre-election audit
    - Check memory card data & programming
    - Check pre-election test procedure results
  - Post-election audit
    - Check memory card data & programming
    - Check post-election status of cards
- Analysis of hand-counted random audit returns

Technological Audit Process

- Engineering and preparation stage
  - Analysis and reverse-engineering when necessary of the voting terminal (VT) hardware and software
    - Customization of software & firmware to extract "all data and information pertaining to election"
    - Byte code safety analysis
  - Development of new software as needed
    - One *cannot* rely on the system to audit *itself*
  - Developing a data collection and analysis tools
- Execution/application stage
  - Data collection (read memory cards) and analysis

Custom Firmware

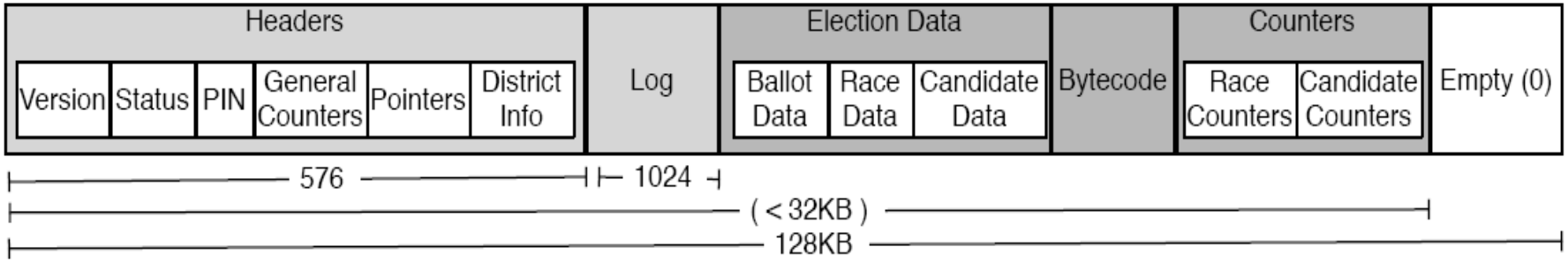
- Custom firmware was developed to escape several major issues with using the native tabulator functions
  - Reliance on the undocumented built-in procedure is questionable
  - Avoid any logging on the memory card
  - Faithfully read the contents of the card
  - Speeding up reading to make audit feasible
- New firmware was developed and deployed for audits
  - *(Note that in itself, this is a successful hardware attack!)*
  - Memory card contents are accurately read with alteration
  - Data delivered through the serial port
  - Speeding up the process by an order of magnitude (streamlining code and using compression)

Data Collection Tool and Methodology

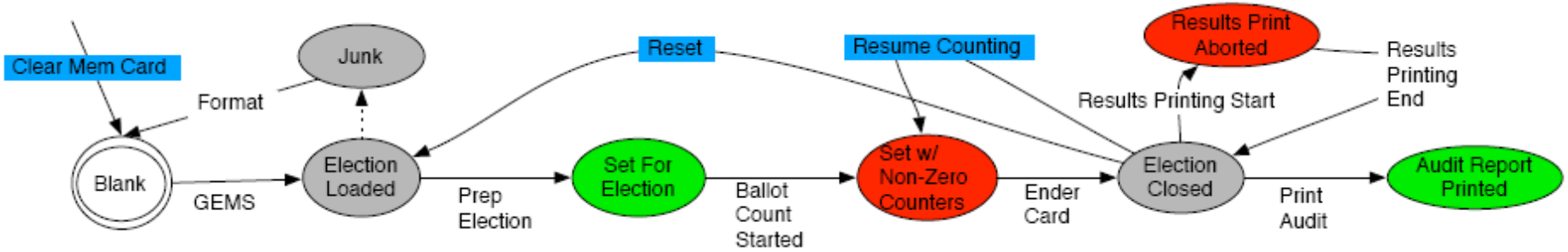
- Testing for data (in)consistency and integrity requires collection of
  - Baseline Data
  - Pre-Election Data from cards
  - Post-Election Data from cards
- Data Collection/Comparison tool
  - Collecting the memory card contents
  - Auditing the collected data by comparing baseline and audit data and analyzing the differences
- Manual byte code analysis

Memory Card Content Analysis

- Our analysis revealed the formatting of the memory



- Memory card audit covers
  - Format, Status, Counters, Elections, Bytecode, Log



Technological Audits in Connecticut

- Technological audit of memory cards
  - Integrity of ballot layout and counters vs. GEMS
  - Bytecode safety:
    counting and printing, no other code
  - Audit log analysis
- Statistical analysis of the hand-counted audit returns
- Reports: http://voter.engr.uconn.edu/voter/

Pre-election Card Audit [2009]

	Cards Usable in the Election		All Cards	
	Number	% Total	Number	% Total
(a) Prior to Use by District				
Good Data, Clean Card	446	99.3%	446	91%
Different Candidate Name	1	0.2%	1	0.2%
Different District Number	1	0.2%	1	0.2%
"Junk" data	0	0%	42	9%
Not Programmed	0	0%	1	0.2%
Totals:	448	100%	491	100%
(b) Phases of Use				
Not Programmed	0	0%	1	0.2%
Not Set for Election	173	39%	173	35%
Set for Election	272	61%	272	56%
Election Closed	3	0.6%	3	0.6%
Preparation Warning	74	16.6%	74	15%
Duplication Events	23	5.1%	23	4.7%
Session Starts	9	2.0%	9	1.8%
Test Election Warning	76	17%	76	15%

Post-election Card Test [2009]

	Cards Used in the Election		All Cards	
	Number	% Total	Number	% Total
(a) Card Format				
Good Data, Clean Card	47	96%	94	78%
Different Elections	0	0%	4	3%
Duplicated Card	2	4%	3	2.5%
(Unusable) Not Programmed	0	0%	2	2%
(Unusable) "Junk data"	0	0%	14	12%
Totals:	49	100%	120	100%
(b) Card Status				
Not Programmed (Blank)	0	0%	2	2%
Not Set for Election	0	0%	6	5.8%
Set for Election	0	0%	45	44%
Election Closed	45	92%	45	38%
Results Print Aborted	4	8%	4	3%

Hand-Counted Audit & Analysis

- 10% audit, randomly selected (for pre-defined races)
- 100% of each selected race is hand counted
- The audit returns are sent to UConn
- UConn alerts SOTS
- SOTS performs follow-up ivestigaiton(s)
- Statistical analysis report is published

Lessons Learned

- Poll workers need to follow the exact testing procedures – this is important!
- Quality issues – memory card failures
  - Up to 15% of all memory cards
  - Follow up Voter Center study determined that weak batteries are the main cause
- The examination of the memory cards revealed no incorrect ballot data or bytecode
- Analysis of hand-counted audit returns
  - Discrepancies are small, with some exceptions
  - In no case can be attributed to machines

96

Current and Planned Work

- Finished technology audit for 2010 primary
- Current work for November 2010 elections
  - Improve memory card audits and test methodology
  - Assist with definition of hand-counted audits
  - Refinement of safe use procedures
- New techniques to improve security/integrity
  - Design experiments to assess optical scan precision
  - Automated comparison analysis of printed ballot
  - Tools for audits and alternate counting in audits
- Firmware evaluation
  - Upgrades to next versions: evaluation and recommendation
  - Firmware safety analysis
- Respond to State needs

Feasibility of Deploying a Solution

- Technical feasibility
  - Many scientists/engineers can justifiably claim:
  - "I can design a better/perfect voting machine!"
  - "I can design a better/perfect election process!"
- Logistics, constraints, and legal issues
  - While many States are scrapping "bleeding edge" machines now, it is not clear it is feasible to implement a nation-wide revamping quickly.
  - If a solution is complex and difficult to present, it will be very hard to deploy through the legislative action
  - Simple and gradual refinements are the best bet
  - Local election experimentation / introduction

Conclusions

- Deployment of new technology
  - Must be methodical, careful, diligent
  - Acknowledging limitations and risks
  - Continuous refinement and improvement
  - Avoid “bleeding” edge adoption risks
- Optical scans are embraced as auditable and relatively safe
  - Do not yet address usability and access issues
  - Need improvements to better capture voter intent
- Futures: new techniques are needed
  - Strengthening onsite overall integrity
  - End-to-end integrity
  - Firmware and bytecode analysis
  - Better audit methodology

Questions and Discussion

Discussion and Questions

- Effective partnership working to ensure technical integrity and security of electoral process
  - Connecticut SOTS Office
  - UCONN VoTeR Center

- Questions?