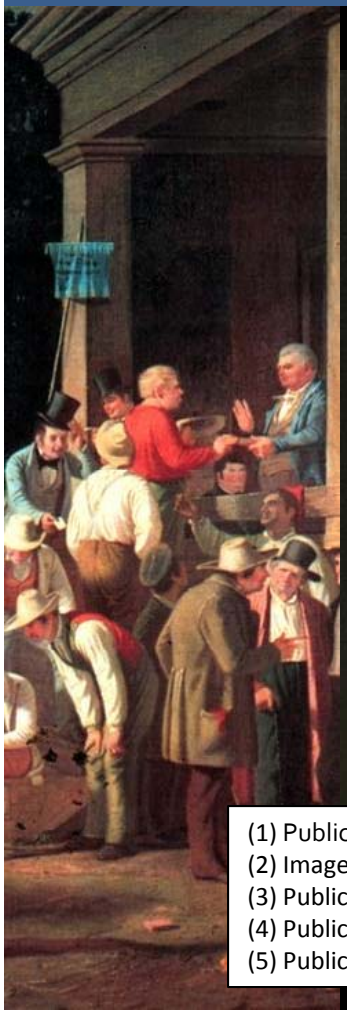
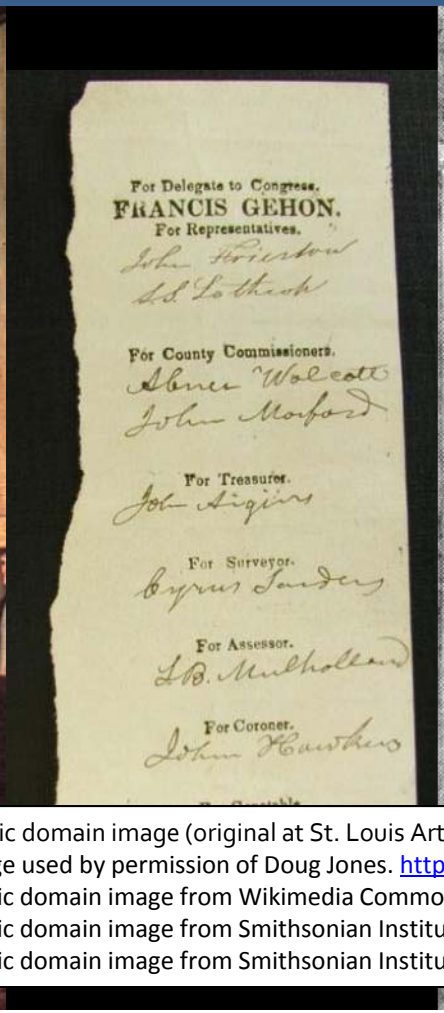
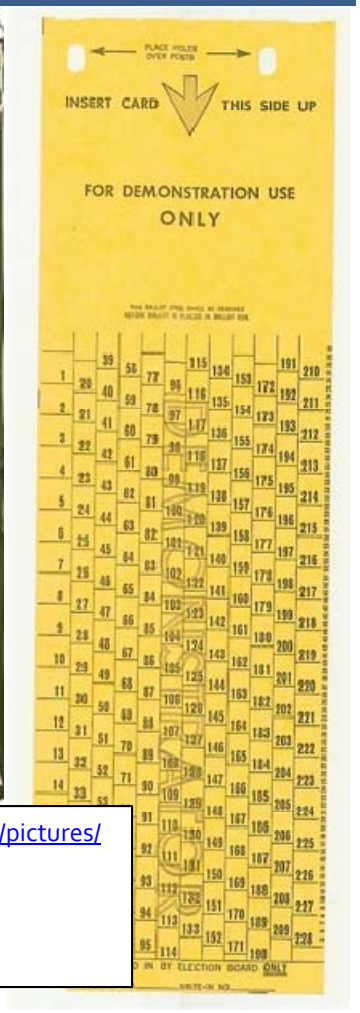
Securing Digital Democracy

Lecture 3 | *Computers at the Polls*

J. Alex Halderman
University of Michigan

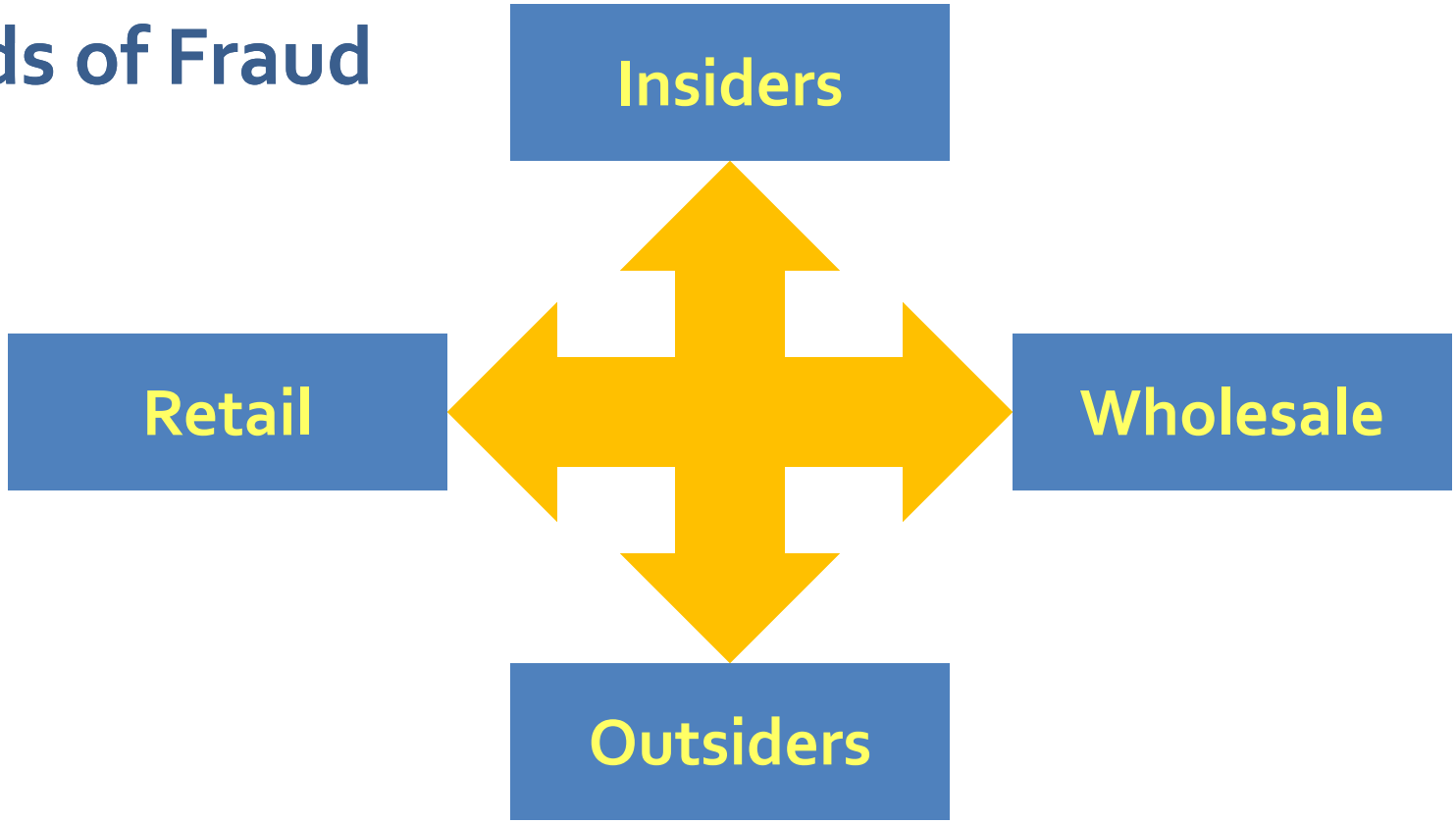






(1) Public domain image (original at St. Louis Art Museum) via Doug Jones. http://homepage.cs.uiowa.edu/~jones/voting/pictures/
(2) Image used by permission of Doug Jones. http://homepage.cs.uiowa.edu/~jones/voting/pictures/
(3) Public domain image from Wikimedia Commons. http://en.wikipedia.org/wiki/File:1900_New_York_polling_place.jpg
(4) Public domain image from Smithsonian Institution. http://americanhistory.si.edu/vote/votingmachine.html
(5) Public domain image from Smithsonian Institution. http://americanhistory.si.edu/vote/punchcard.html

Kinds of Fraud

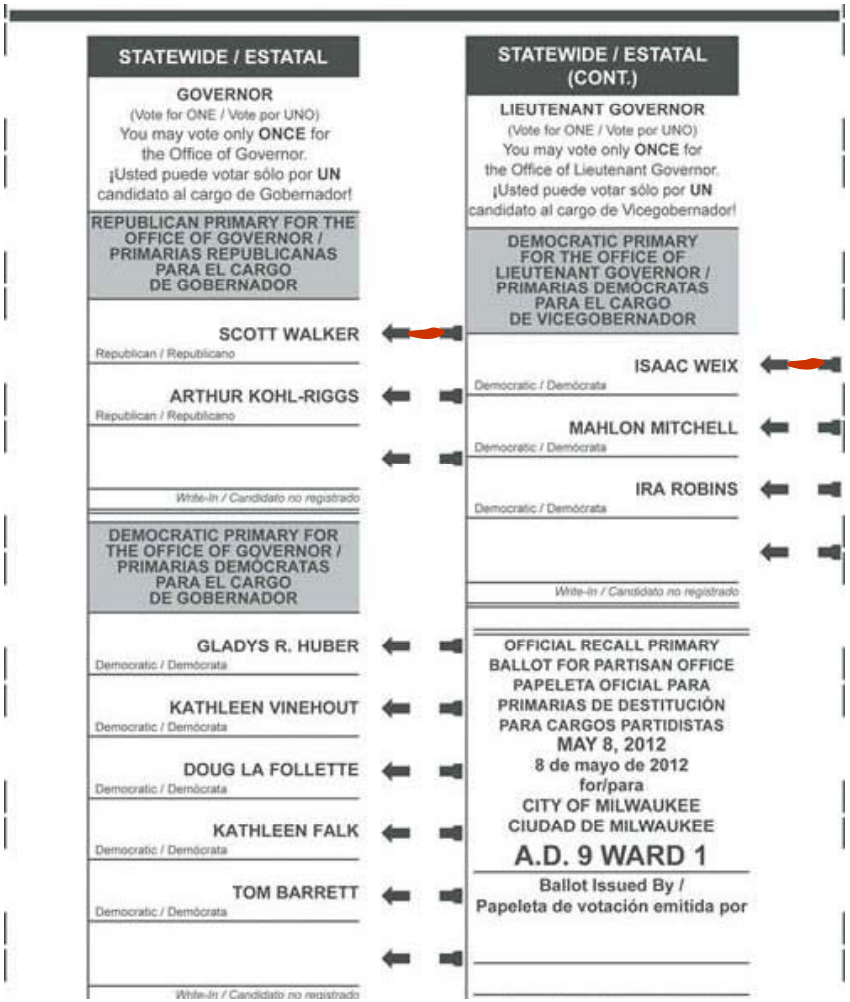


DREs **Optical Scan** = **Computers**

(1), (2) Public domain images from Smithsonian Institution. http://americanhistory.si.edu/vote/future.htm

Optical Scan Voting

(left) Public domain image from Smithsonian Institution. http://americanhistory.si.edu/vote/patchwork.html
(right) Public domain image from Smithsonian Institution. http://americanhistory.si.edu/vote/future.htm



STATEWIDE / ESTATAL

GOVERNOR
(Vote for ONE / Vote por UNO)
You may vote only ONCE for the Office of Governor.
¡Usted puede votar sólo por UN candidato al cargo de Gobernador!

REPUBLICAN PRIMARY FOR THE OFFICE OF GOVERNOR / PRIMARIAS REPUBLICANAS PARA EL CARGO DE GOBERNADOR

SCOTT WALKER
Republican / Republicano

ARTHUR KOHL-RIGGS
Republican / Republicano

Write-In / Candidato no registrado

DEMOCRATIC PRIMARY FOR THE OFFICE OF GOVERNOR / PRIMARIAS DEMÓCRATAS PARA EL CARGO DE GOBERNADOR

GLADYS R. HUBER
Democratic / Demócrata

KATHLEEN VINEHOUT
Democratic / Demócrata

DOUG LA FOLLETTE
Democratic / Demócrata

KATHLEEN FALK
Democratic / Demócrata

TOM BARRETT
Democratic / Demócrata

Write-In / Candidato no registrado

STATEWIDE / ESTATAL (CONT.)

LIEUTENANT GOVERNOR
(Vote for ONE / Vote por UNO)
You may vote only ONCE for the Office of Lieutenant Governor.
¡Usted puede votar sólo por UN candidato al cargo de Vicegobernador!

DEMOCRATIC PRIMARY FOR THE OFFICE OF LIEUTENANT GOVERNOR / PRIMARIAS DEMÓCRATAS PARA EL CARGO DE VICEGOBERNADOR

ISAAC WEIX
Democratic / Demócrata

MAHLON MITCHELL
Democratic / Demócrata

IRA ROBINS
Democratic / Demócrata

Write-In / Candidato no registrado

OFFICIAL RECALL PRIMARY BALLOT FOR PARTISAN OFFICE
PAPELETA OFICIAL PARA PRIMARIAS DE DESTITUCIÓN PARA CARGOS PARTIDISTAS
MAY 8, 2012
8 de mayo de 2012
for/para
CITY OF MILWAUKEE
CIUDAD DE MILWAUKEE
A.D. 9 WARD 1
Ballot Issued By /
Papeleta de votación emitida por

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 canc 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. T the OVAL next to the word "Yes" or the word "No". All distinguishing marks or erasures are forbidden and make the ballo wrongly mark this ballot, return it and get another. VOTE LIKE THIS: ● VOTE BOTH SIDES

STATE

GOVERNOR
Vote for One

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

LIEUTENANT GOVERNOR
Vote for One

- ○ PAT WRIGHT — Libertarian — Ferret Legalization Coordinator
- ○ PAUL JERRY HANNOSH — Reform — Educator/Businessman
- ○ BRUCE MC PHERSON — Republican — California State Senator
- ○ KALEE PRZYBYLAK — Natural Law — Public Relations Director
- ○ CRUZ M. BUSTAMANTE — Democratic — Lieutenant Governor
- ○ JIM KING — American Independent

INSURANCE COMMISSIONER
Vote for One

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

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

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

UNITED STATES REPRESENTATIVE
24TH District

FOR ASSOCIATE 2nd APPELLAT

Shall ASSOCIAT ASHMANN be ele prescribed by law

○ YES

FOR ASSOCIATE 2nd APPELLAT

FOR ASSOCIATE 2nd APPELLAT

Shall ASSOCIAT TODD be elected prescribed by law

○ YES

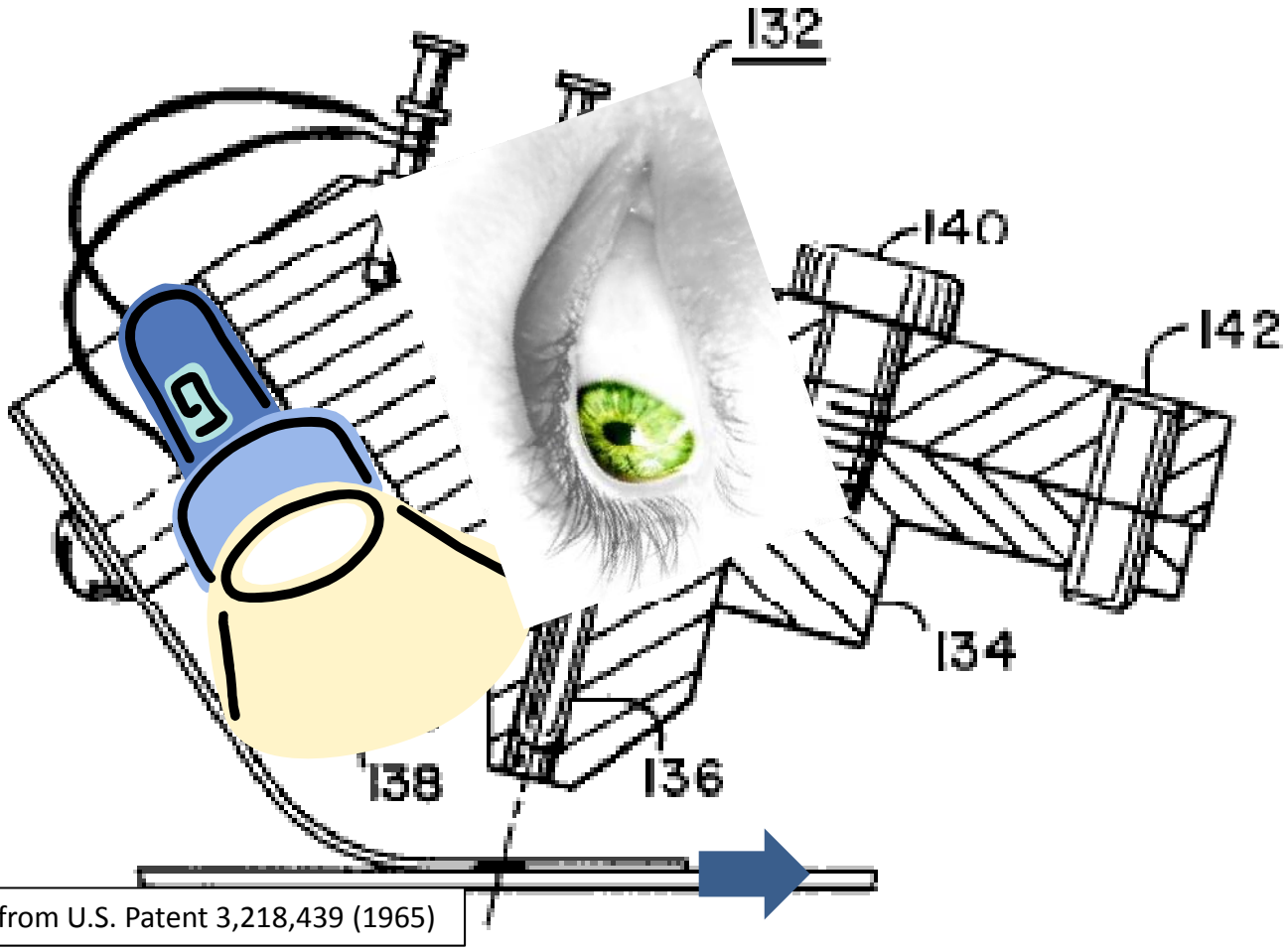
FOR PRESIDING 2nd APPELLATE

Shall PRESIDING KLEIN be elected prescribed by law

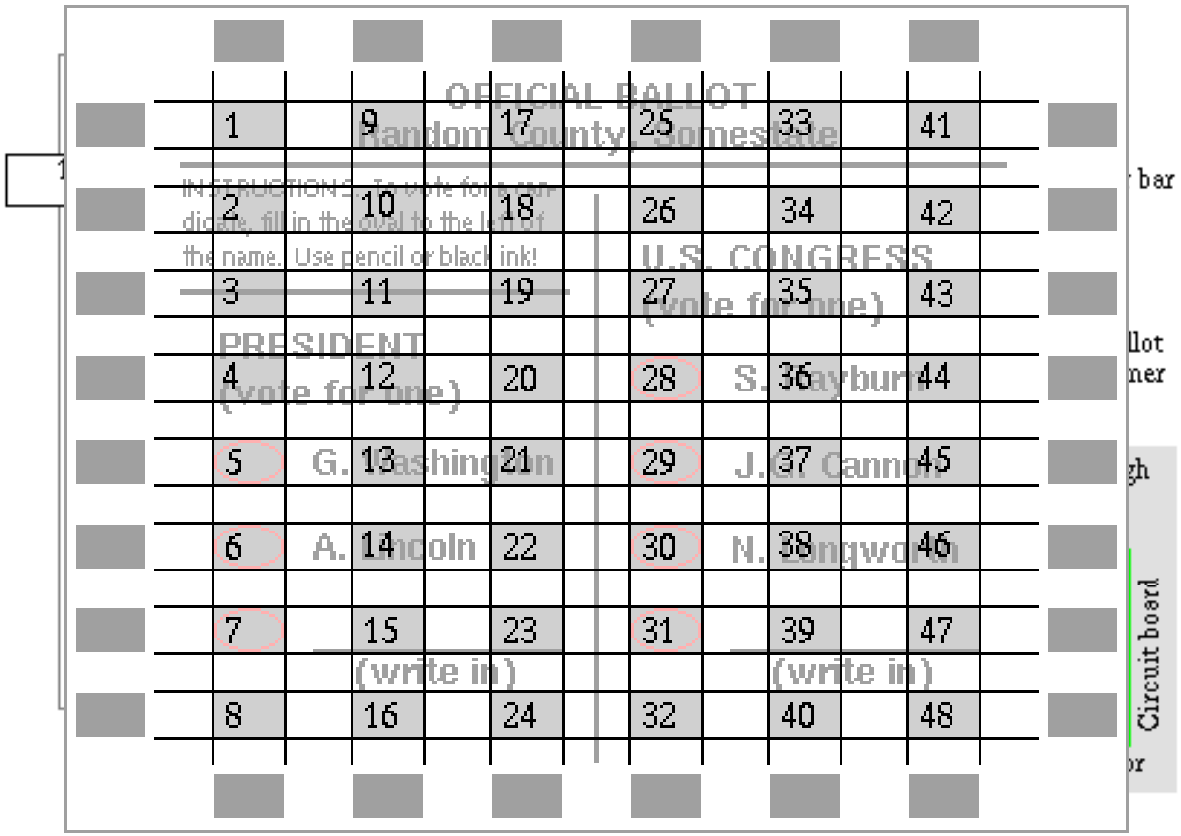
○ YES

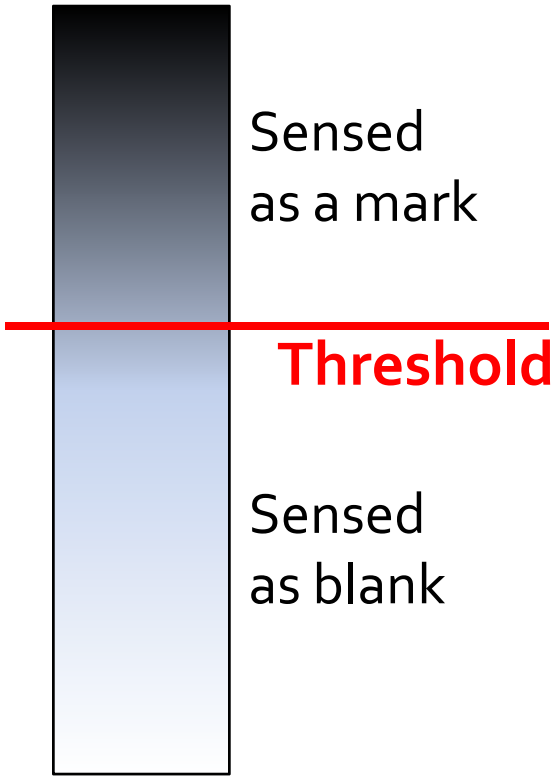
FOR ASSOCIATE 2nd APPELLAT

Shall ASSOCIAT

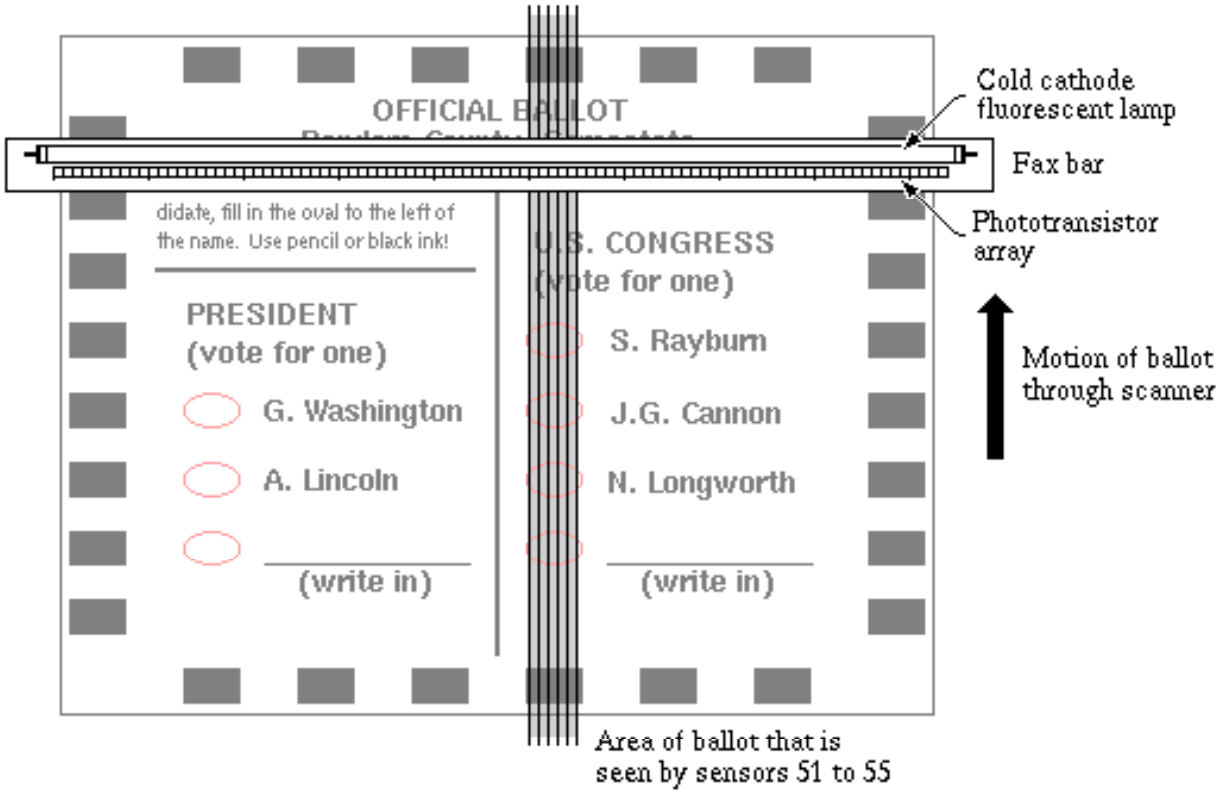


Public domain image from U.S. Patent 3,218,439 (1965)





Diagrams (left) by Doug Jones. http://homepage.cs.uiowa.edu/~jones/voting/optical/



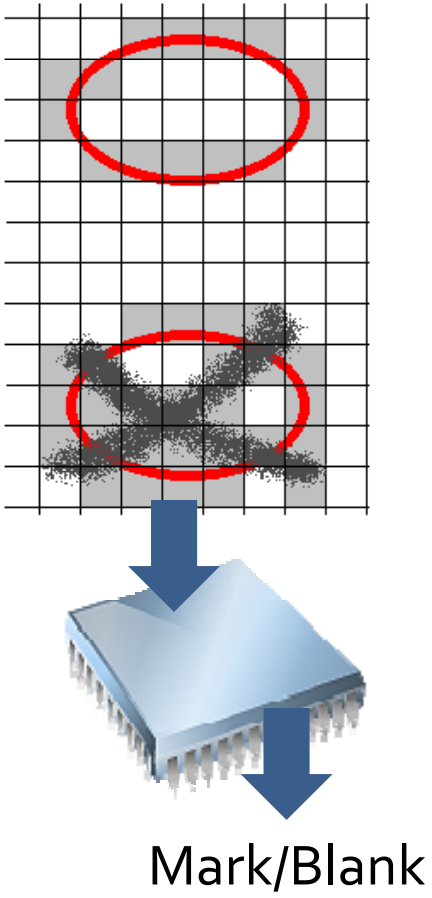
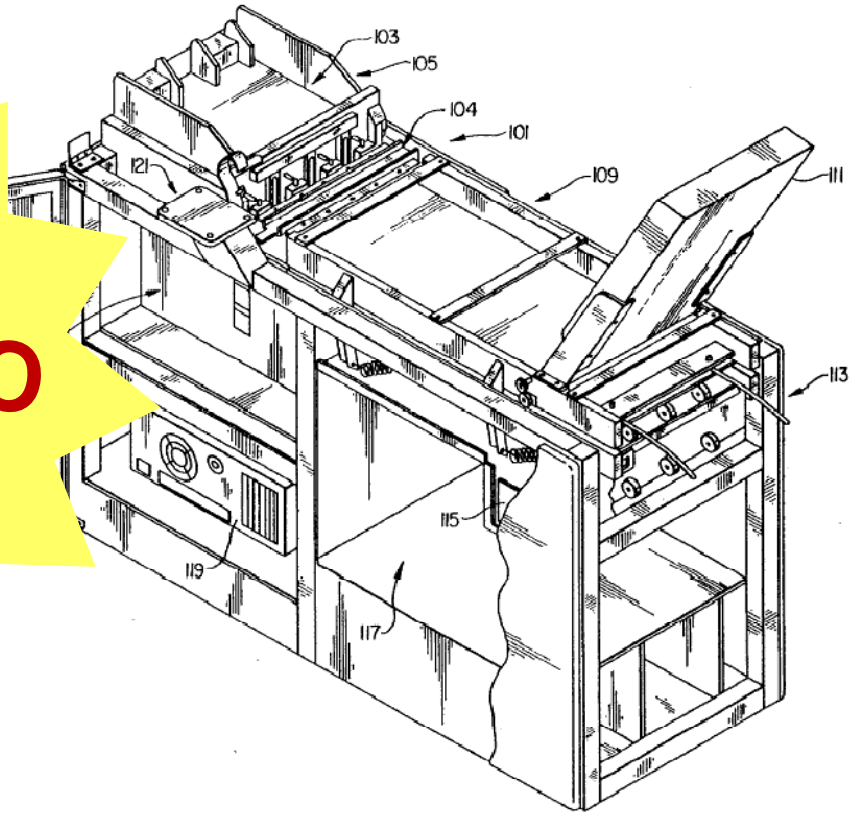


Diagram by Doug Jones. http://homepage.cs.uiowa.edu/~jones/voting/optical/

WHAT COULD GO WRONG?



Precinct Count

Central Count

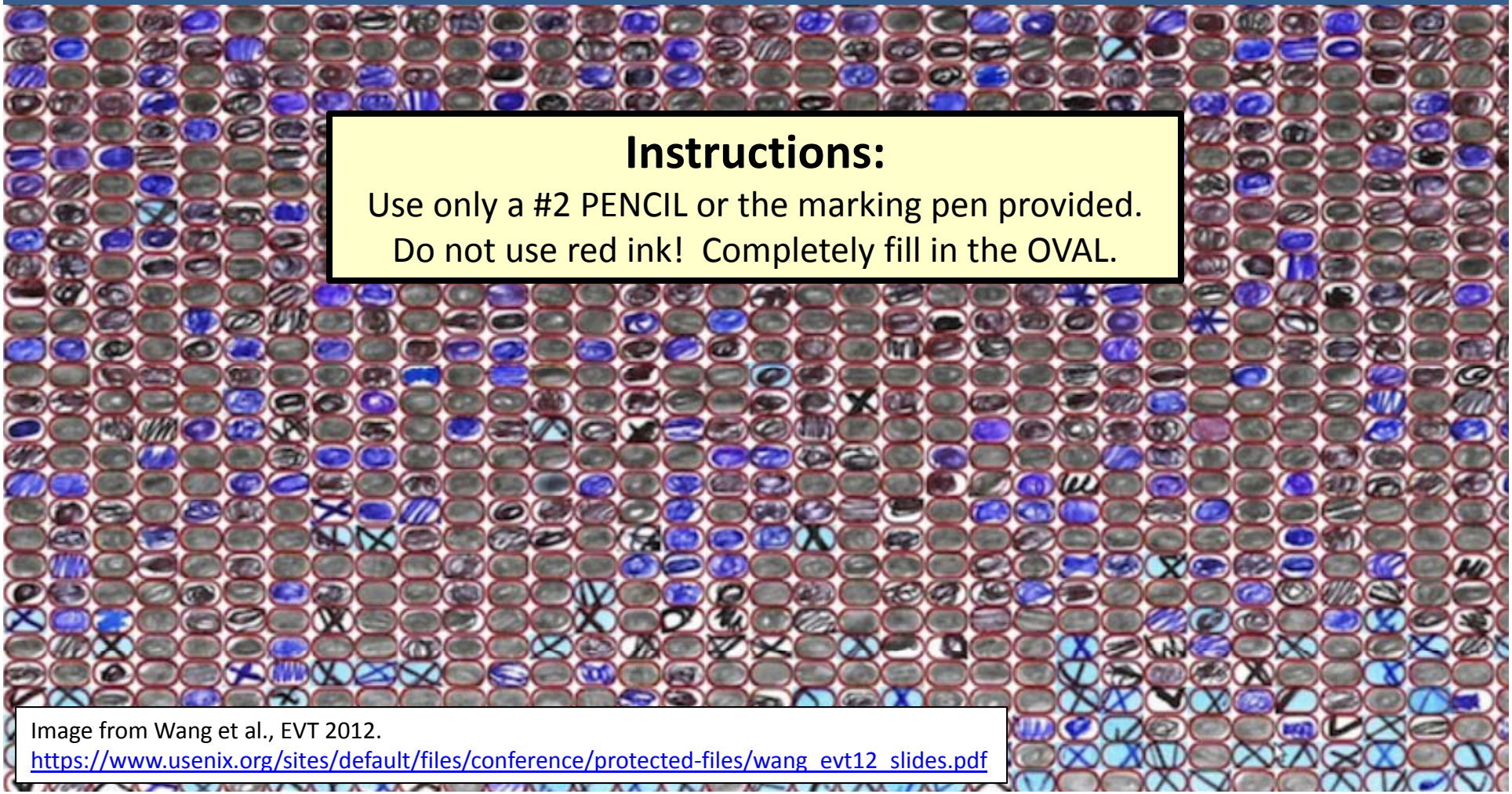
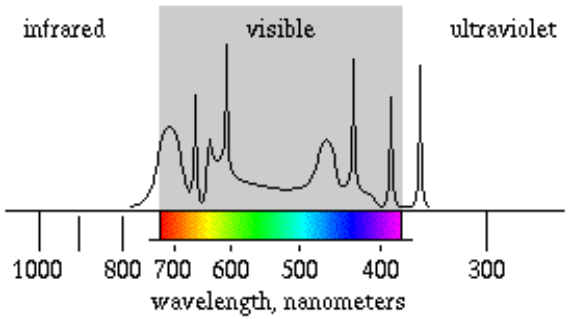
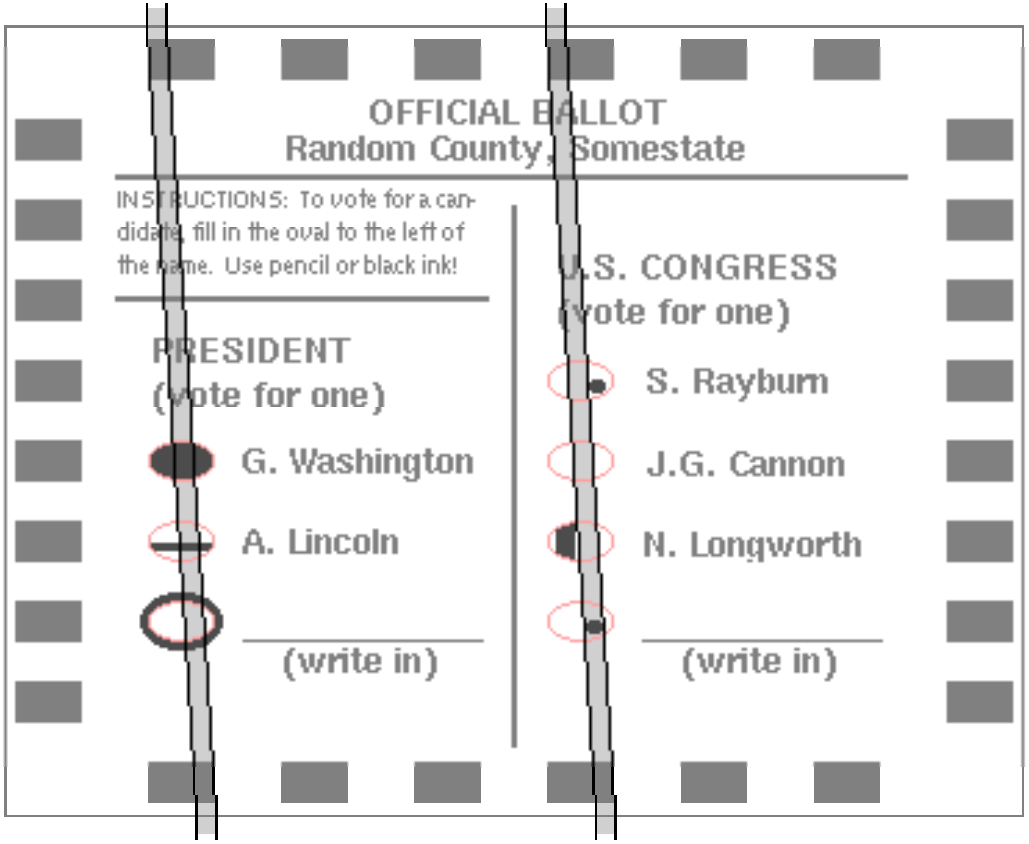


Image from Wang et al., EVT 2012.
https://www.usenix.org/sites/default/files/conference/protected-files/wang_evt12_slides.pdf





Illustrations by Doug Jones. http://homepage.cs.uiowa.edu/~jones/voting/optical/

Bubble Trouble: Off-Line De-Anonymization of Bubble Forms

Abstract

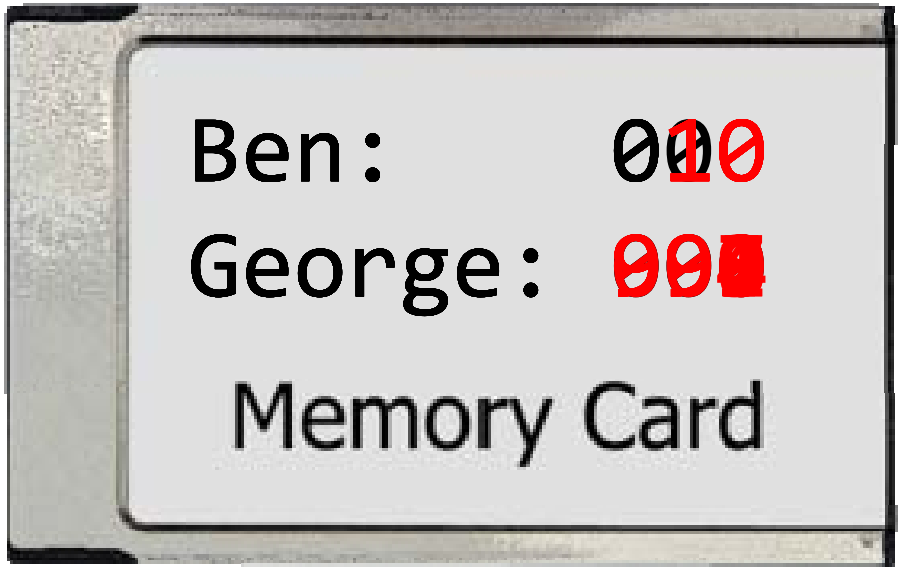
Fill-in-the-bubble forms are widely used for surveys, election ballots, and standardized tests. In these and other scenarios, use of the forms comes with an implicit assumption that individuals' bubble markings themselves are not identifying. This work challenges this assumption, demonstrating that fill-in-the-bubble forms could convey a respondent's identity even in the absence of explicit identifying information. We develop methods to capture the unique features of a marked bubble and use machine learning to isolate characteristics indicative of its creator. Using surveys from more than ninety indi-

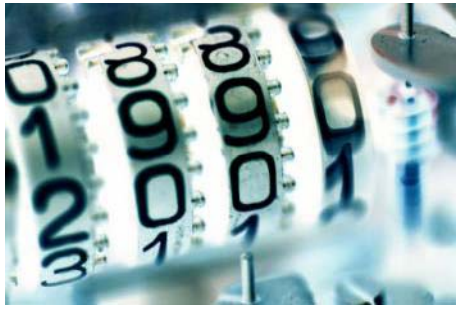
tential implications, from detecting cheating on standardized tests to threatening the anonymity of election ballots.

Bubble forms are widely used in scenarios where confirming or protecting the identity of respondents is critical. Over 137 million registered voters in the United States reside in precincts with optical scan voting machines [27], which traditionally use fill-in-the-bubble paper ballots. Voter privacy (and certain forms of fraud) relies on an inability to connect voters with these ballots. Surveys for research and other purposes use bubble forms to automate data collection. The anonymity of survey subjects not only affects subject honesty but also impacts requirements governing human subjects research [26]. Over 1.6 million members of the high school class of 2010 completed the SAT [8], one of many large-

Calandrino, et al. Usenix Security 2011. Available at http://www.cs.princeton.edu/~jcalandr/papers/bubbles-usenix11.pdf


15741
15737
15742
15738
Harri Hursti

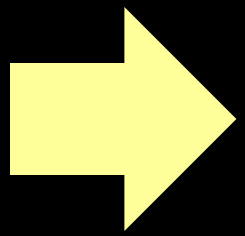

Ben: 010
George: 001
Memory Card



DRE Voting Machines

Direct Recording Electronic

3.3 DRE Voting Machines



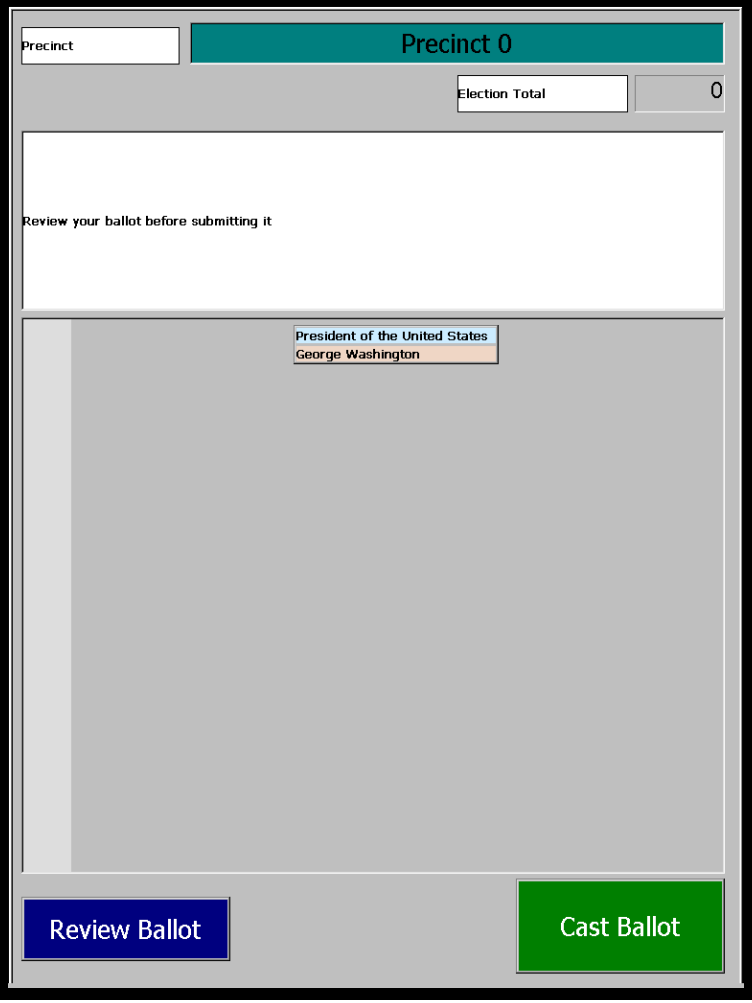
Public domain image from Smithsonian Institution.
http://americanhistory.si.edu/vote/future.html


DIEBOLD

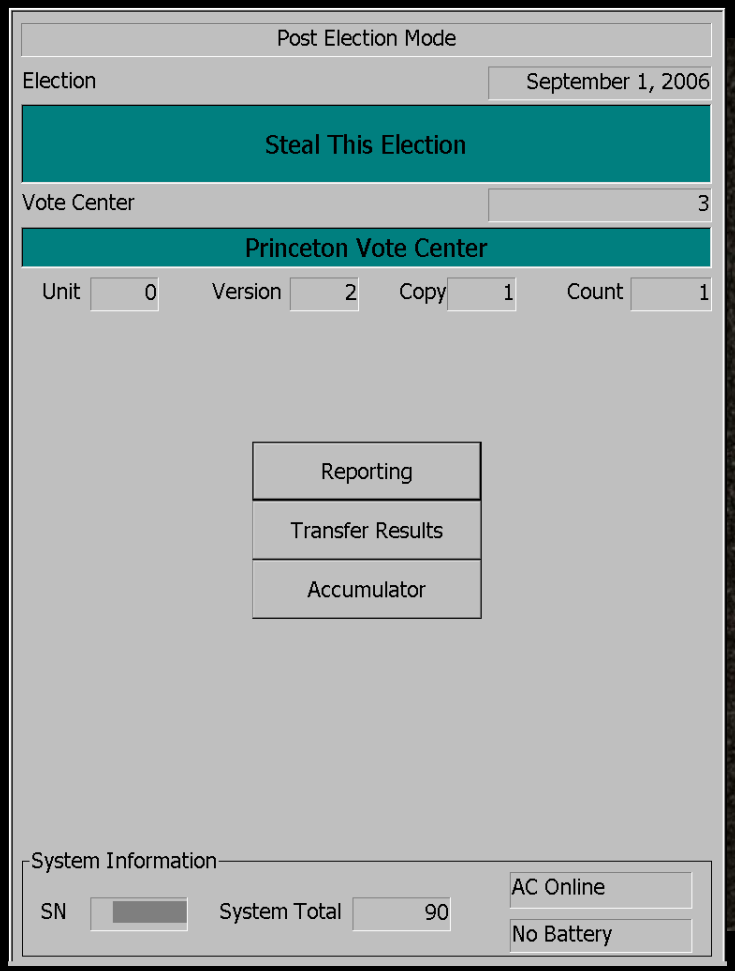

DIEBOLD

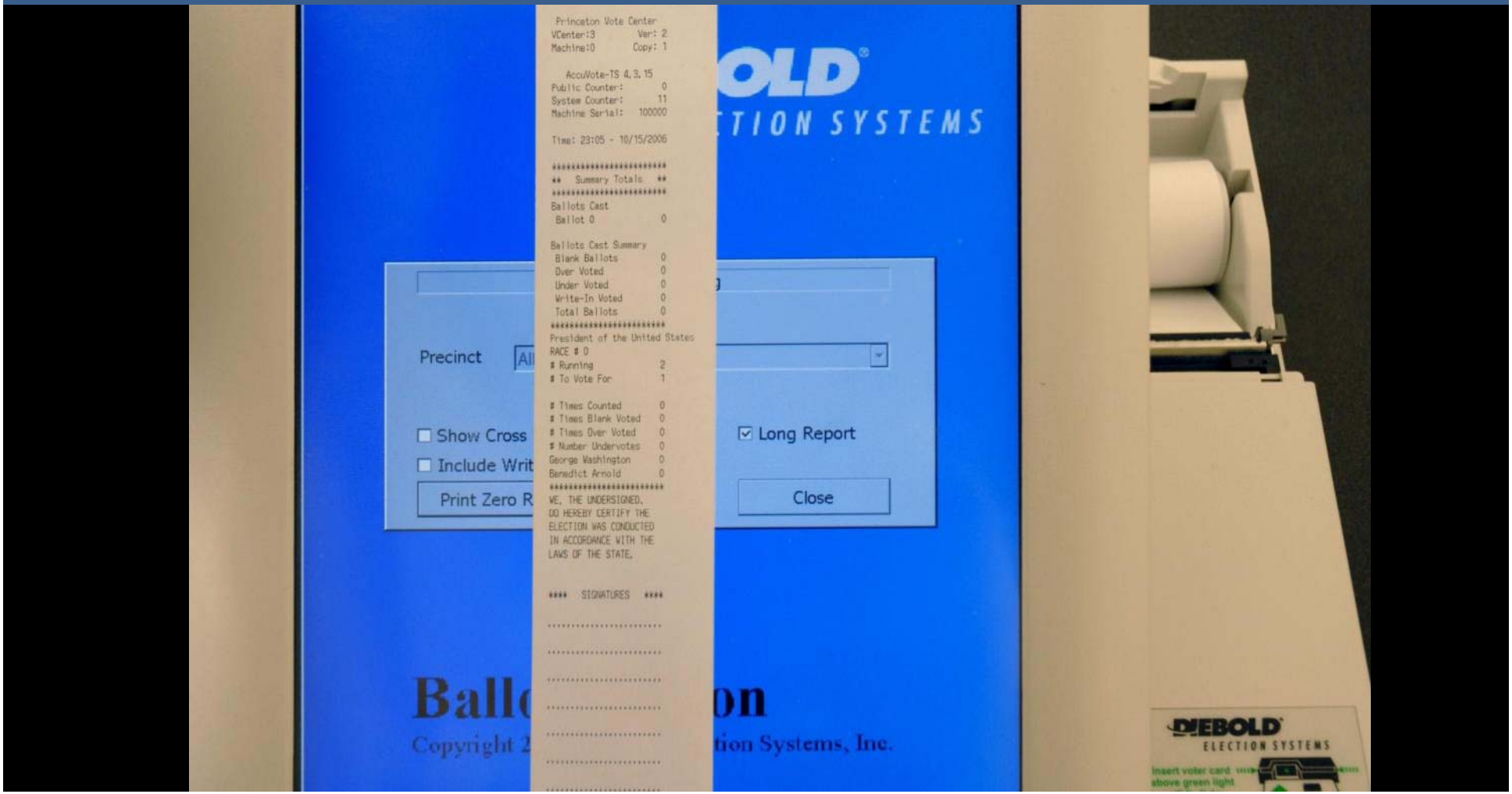

Voter Access Card

Public domain image from Smithsonian Institution.
http://americanhistory.si.edu/vote/future.html

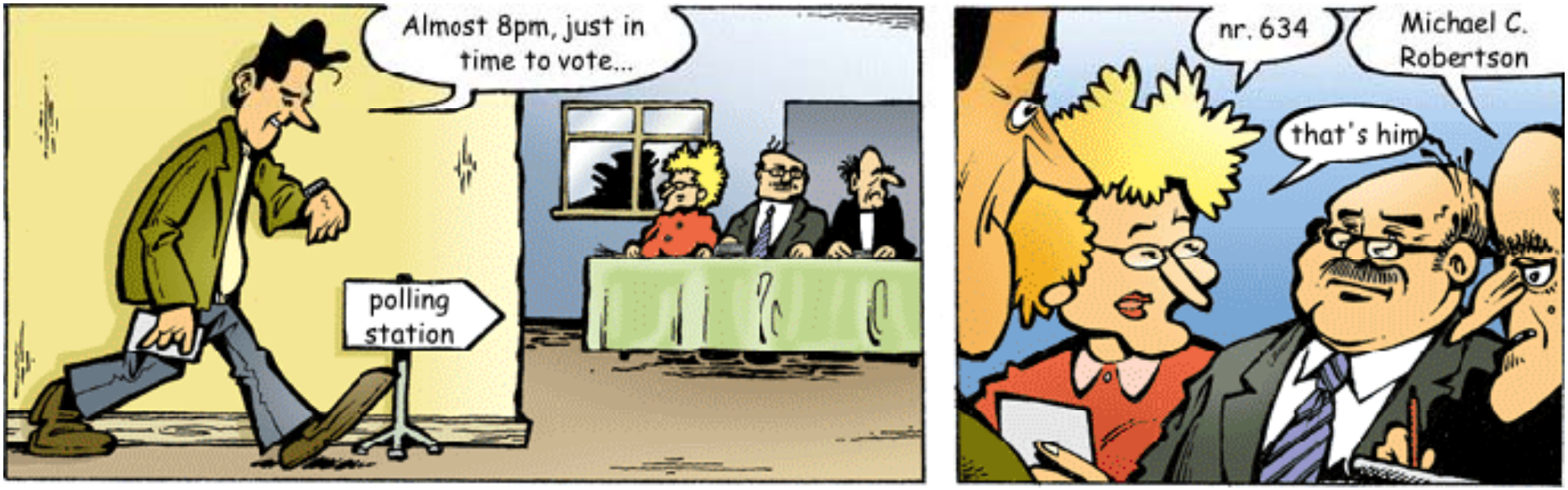

Precinct
Precinct 0
Election Total
0
Review your ballot before submitting it
President of the United States
George Washington
Review Ballot
Cast Ballot

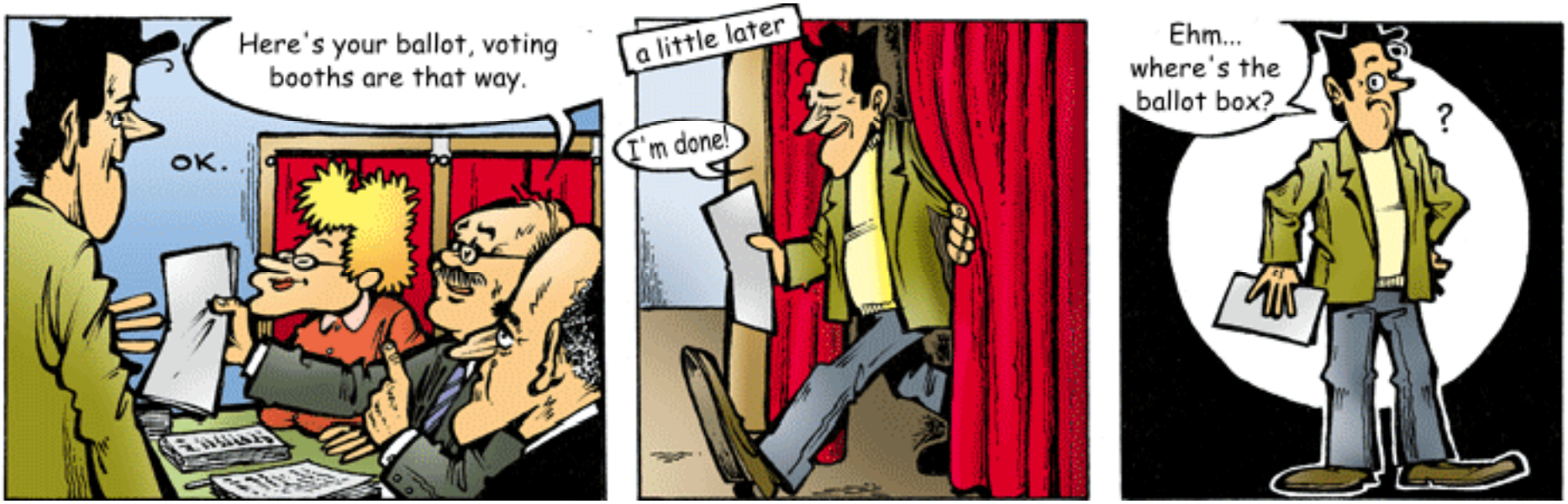
3.3 DRE Voting Machines

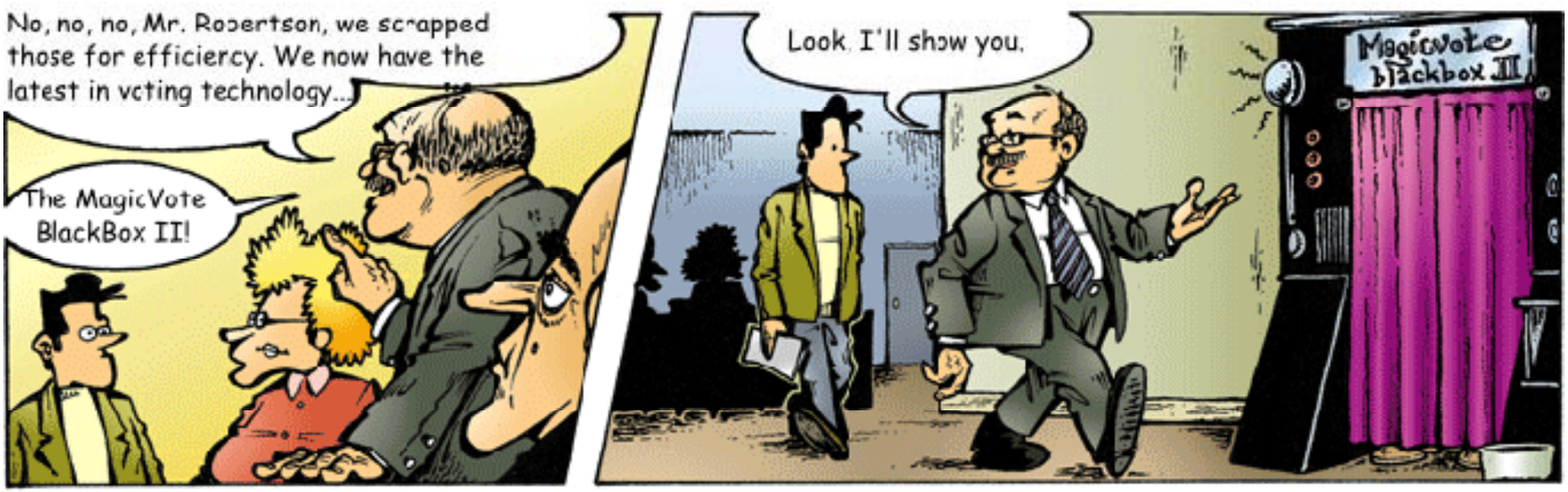


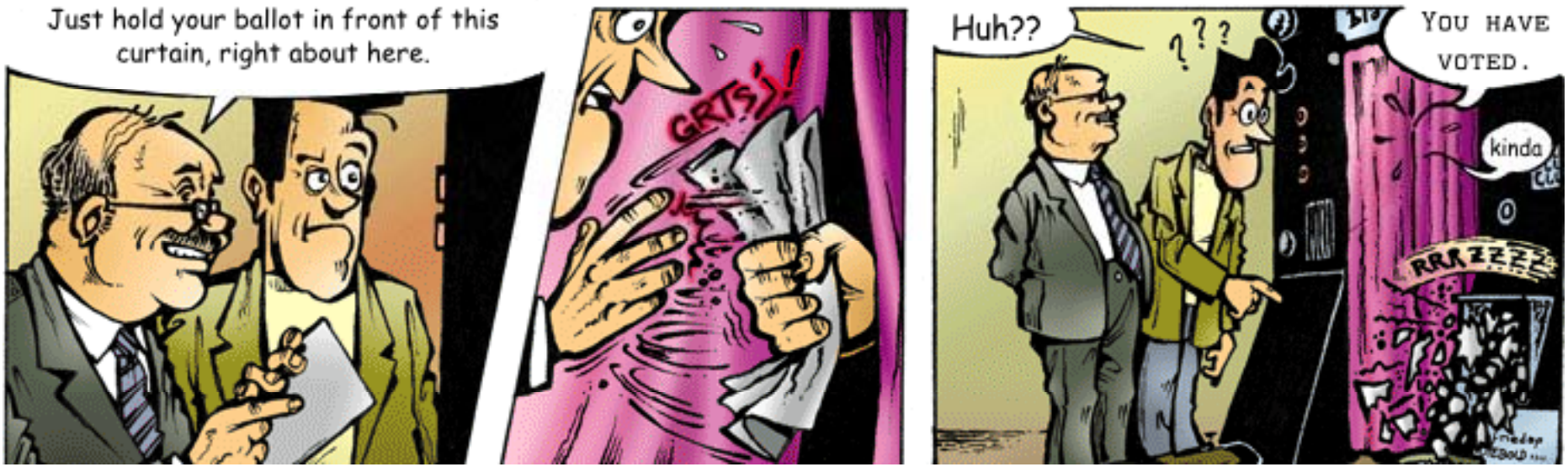

Princeton Vote Center
VCenter:3 Ver: 2
Machine:0 Copy: 1
AccuVote-TS 4.3.15
Public Counter: 0
System Counter: 11
Machine Serial: 100000
Time: 23:05 - 10/15/2006
** Summary Totals **
Ballots Cast
Ballot 0 0
Ballots Cast Summary
Blank Ballots 0
Over Voted 0
Under Voted 0
Write-In Voted 0
Total Ballots 0
President of the United States
RACE # 0
Running 2
To Vote For 1
Times Counted 0
Times Blank Voted 0
Times Over Voted 0
Number Undervotes 0
George Washington 0
Benedict Arnold 0
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
LAWS OF THE STATE.
**** SIGNATURES ****
Precinct
Show Cross
Include Writ
Print Zero R
Long Report
Close
TION SYSTEMS
Copyright
tion Systems, Inc.
DIEBOLD
ELECTION SYSTEMS
Insert voter card
above green light

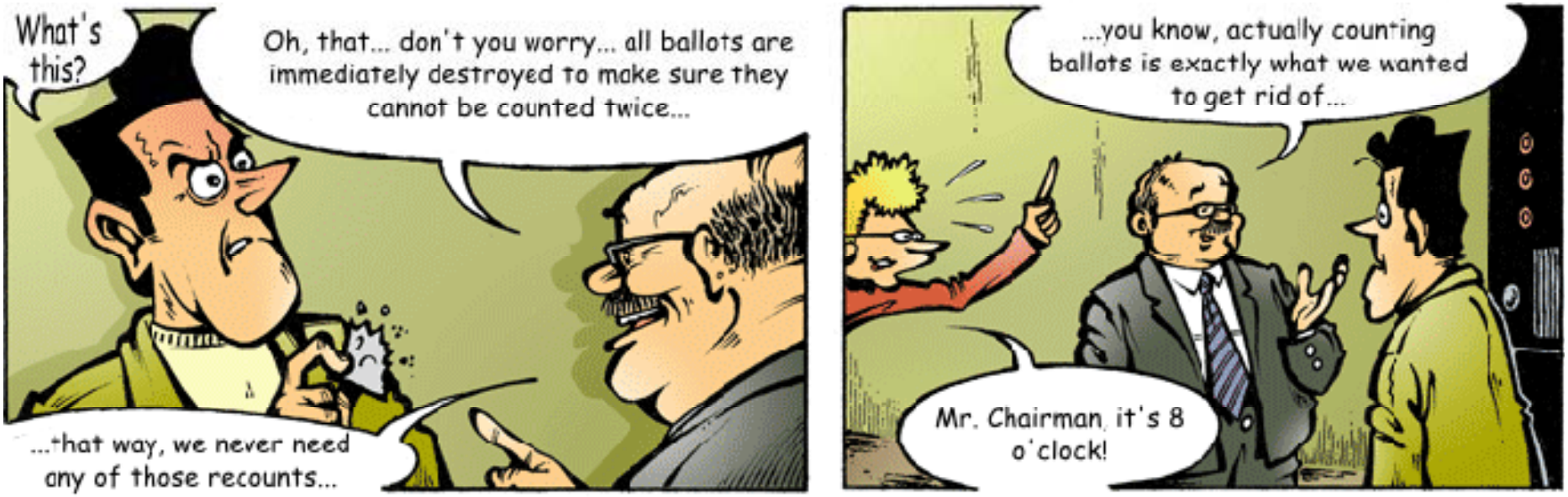
WHAT COULD GO WRONG?

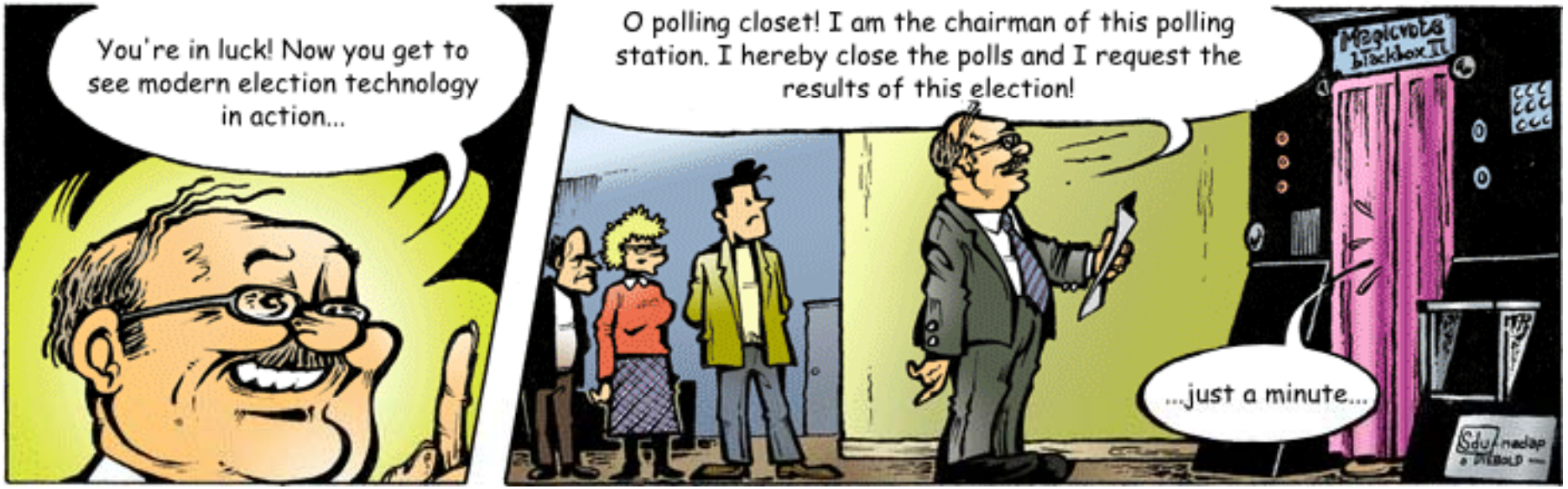


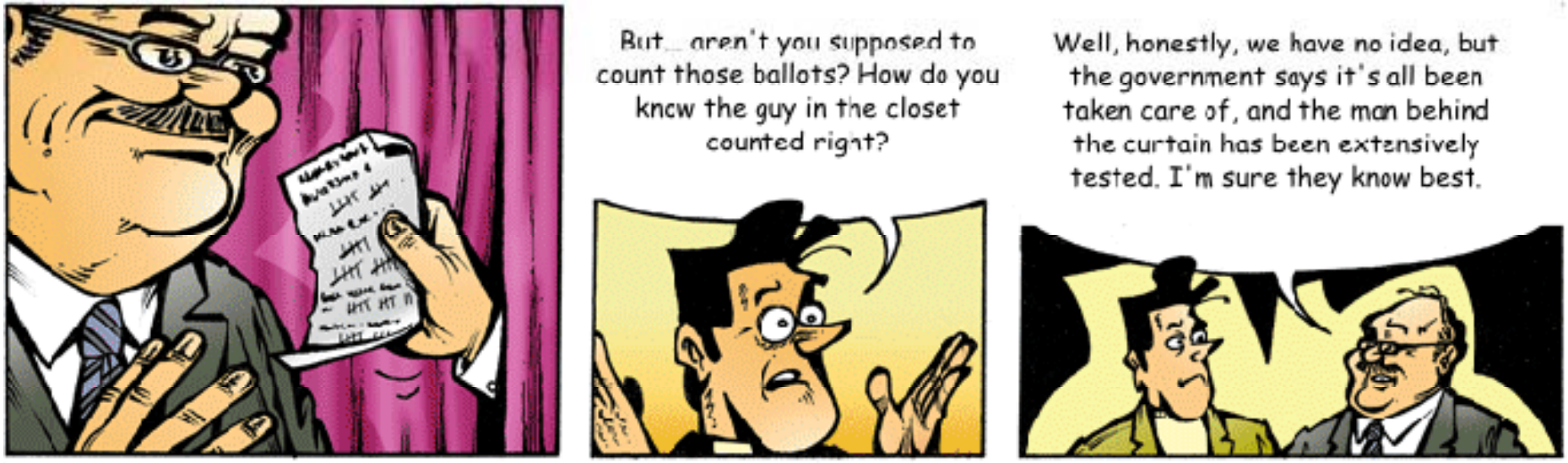

Here's your ballot, voting booths are that way.
OK.
a little later
I'm done!
Ehm... where's the ballot box?
?

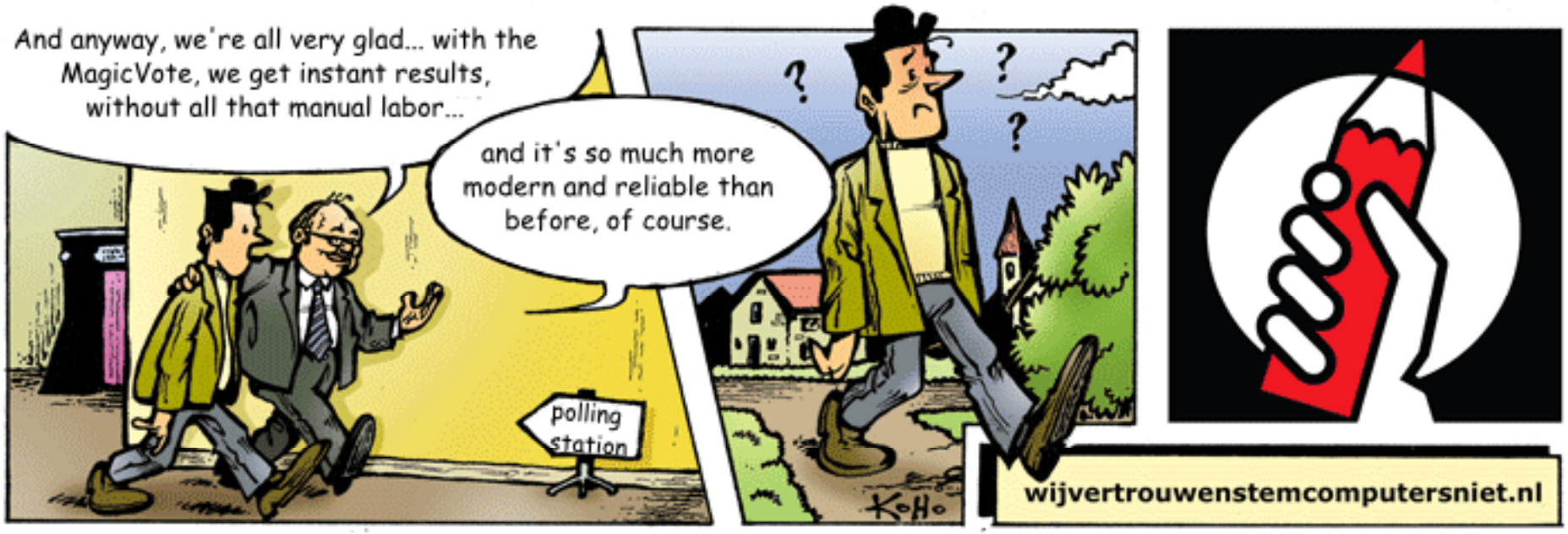

No, no, no, Mr. Robertson, we scrapped those for efficiercy. We now have the latest in vcting technology...
The MagicVote BlackBox II!
Look. I'll shcw you.
MagicVote BlackBox II


Just hold your ballot in front of this curtain, right about here.
GRTS!
Huh??
YOU HAVE VOTED.
kinda
RRRZZZZ


What's this?
Oh, that... don't you worry... all ballots are immediately destroyed to make sure they cannot be counted twice...
...that way, we never need any of those recounts...
...you know, actually counting ballots is exactly what we wanted to get rid of...
Mr. Chairman, it's 8 o'clock!


You're in luck! Now you get to see modern election technology in action...
O polling closet! I am the chairman of this polling station. I hereby close the polls and I request the results of this election!
...just a minute...


But... aren't you supposed to count those ballots? How do you know the guy in the closet counted right?
Well, honestly, we have no idea, but the government says it's all been taken care of, and the man behind the curtain has been extensively tested. I'm sure they know best.



Drawings: Koen Hottentot — Story: Rop Gonggrijp / Barry Wels — Color: Adam Swiecky — Translation: Jaap Weel

Hard Problem: Correct Software

Even Harder: Secure Software

Even Harder: Secure Software for Voting

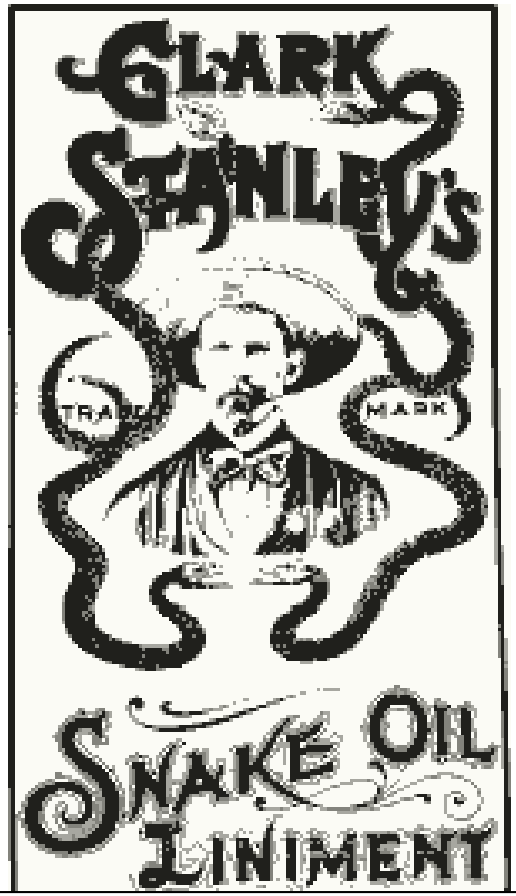
Integrity  Ballot Secrecy

Trustworthy Technology?

Errors?	Vulnerabilities?	System Integrity?
Design Flaws	Software Security	Secret Software
Software Bugs	Hardware Sabotage	Unapproved Software
Hardware Glitches	Data Manipulation	COTS Software
Reliability Problems	Privacy Leaks	Dishonest Lookalikes

Inside the Black Box

Secret Software



(center) Public domain image from Wikimedia Commons. http://en.wikipedia.org/wiki/File:Snake-oil.png

Analysis of an Electronic Voting System

TADAYOSHI KOHNO* ADAM STUBBLEFIELD† AVIEL D. RUBIN‡
DAN S. WALLACH§

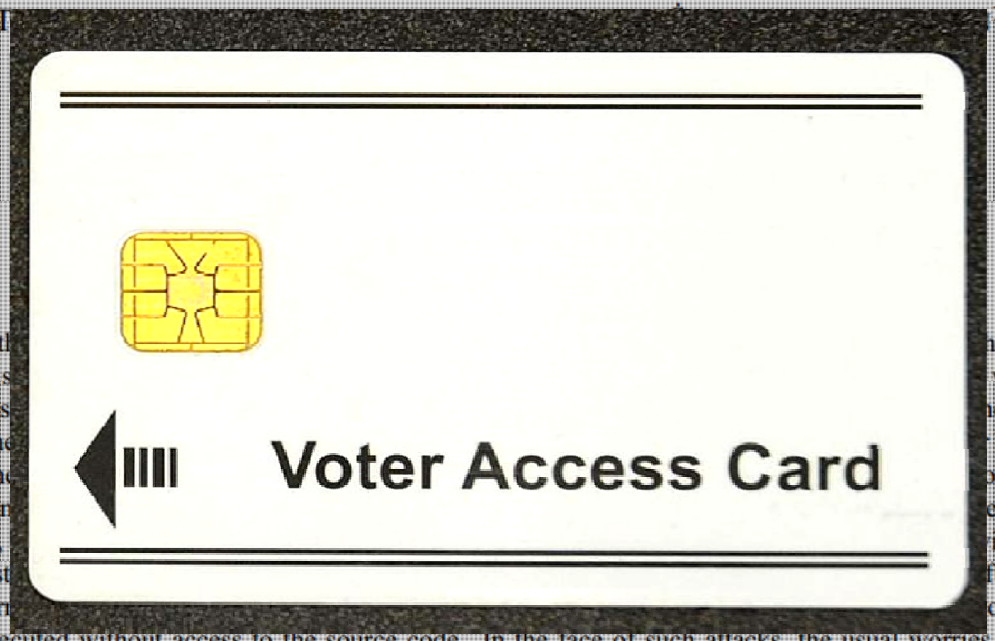
February 27, 2004

Abstract

With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Furthermore, we show that even the most serious of our outsider attacks could have been discovered [illegible]e source code. In the face of such attacks, the usual worries about [illegible]ncerns; outsiders can do the damage. That said, we demonstrate that [illegible]siderable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who

Kohno, et al. IEEE Symp. on Security and Privacy, 2004. Available at http://avirubin.com/vote.pdf

Analysis of an Electronic Voting System



and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker,

Analysis of an Electronic Voting System

Tadayoshi Kohno* Adam Stubblefield† Aviel D. Rubin‡

Encryption

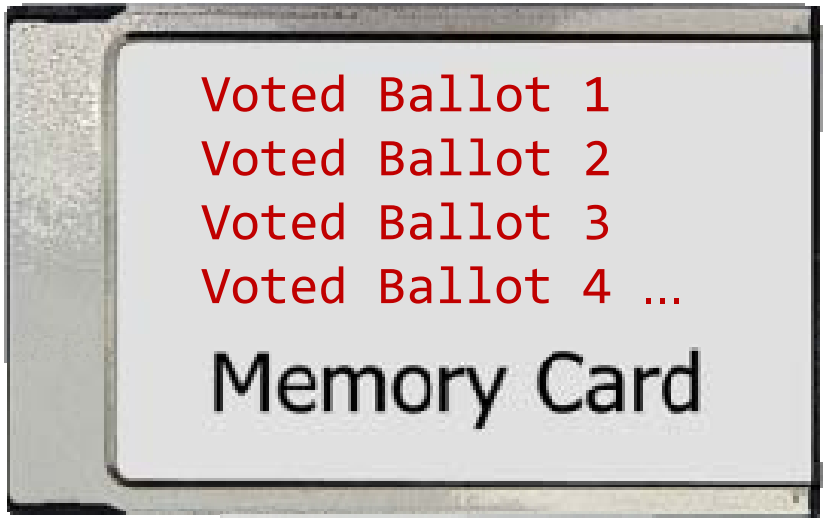
```
#define DESKEY ((des_key*)"F2654hD4")
```

Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who

Analysis of an Electronic Voting System

TADAYOSHI KOHNO* ADAM STUBBLEFIELD† AVIEL D. RUBIN‡

Ballot Secrecy



Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who

Analysis of an Electronic Voting System

Engineering Practices

```
/* Okay, I don't like this one bit. Its really tough
to tell where m_AudioPlayer should live. [...] A
reorganization might be in order here. */

/* This is a bit of a hack for now. [...] Calling
from the timer message appears to work. Solution is
to always do a 1ms wait between audio clips. */

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

the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker,

Analysis of an Electronic Voting System

TADAYOSHI KOHNO* ADAM STUBBLEFIELD† AVIEL D. RUBIN‡
DAN S. WALLACH§

February 27, 2004

Abstract

With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who

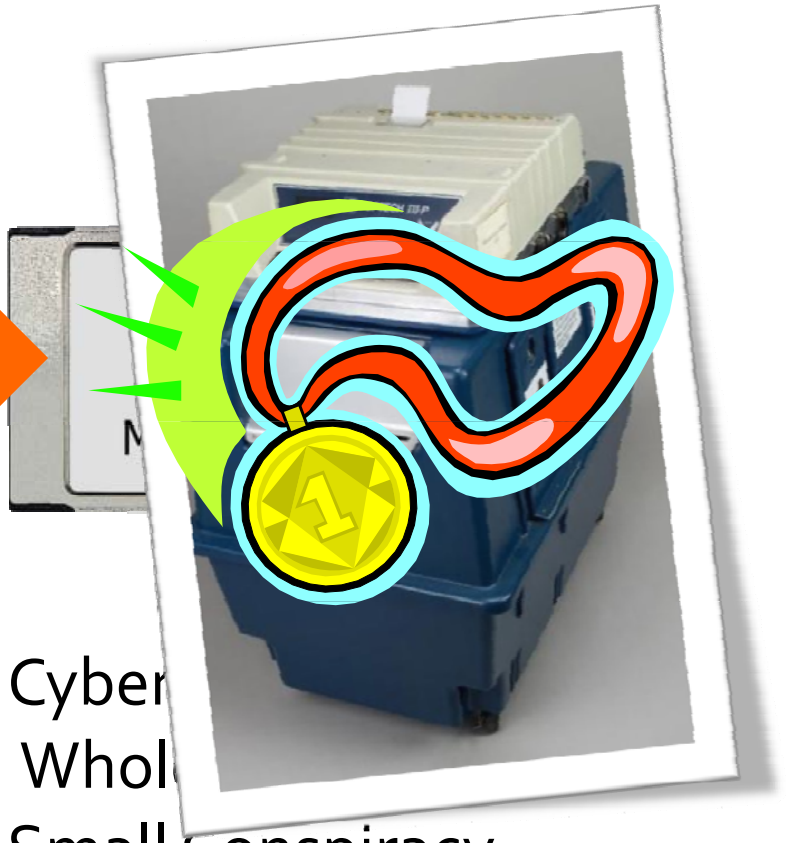
Spot the Security Bug?

```
// Check to see if there is an installation file on the storage card
WIN32_FIND_DATA findData;
HANDLE hFind = ::FindFirstFile(_T("\\Storage Card\\*.ins"), &findData);
if (hFind != INVALID_HANDLE_VALUE) {
    do {
        TCHAR name;
        _stprintf(&name, _T("\\Storage Card\\%s"), findData.cFileName);
        Install(&name, hInstance);
    }
    while (::FindNextFile(hFind, &findData));
    CloseHandle(hFind);
}
```

Paper as a Defense

Redundant Records

AUDIT =?



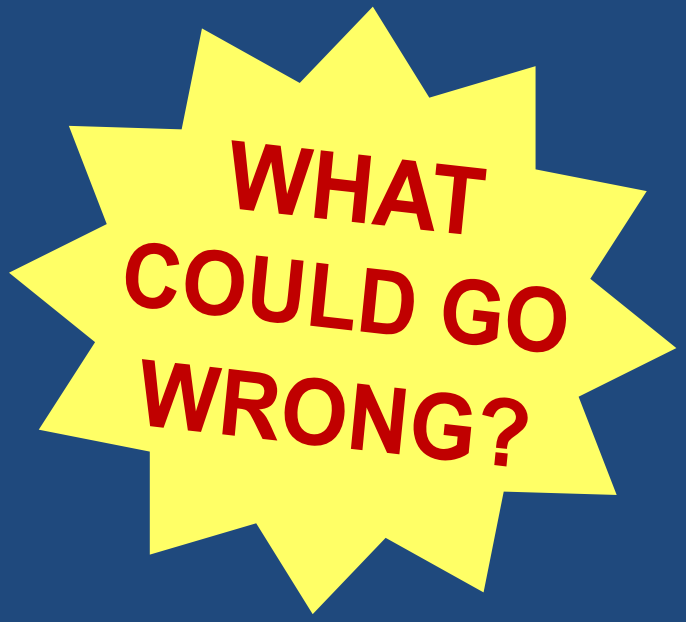
Physical tampering
Retail fraud
Large Conspiracy

Cyber
Whol
Small Conspiracy

DRE+VVPAT

Voter-Verifiable Paper Audit Trail

Voter-Verified Physical Audit Trail



Securing Digital Democracy

Lecture 3 | *Computers at the Polls*

J. Alex Halderman
University of Michigan