Electronic Voting

CS 161: Computer Security

Prof. David Wagner

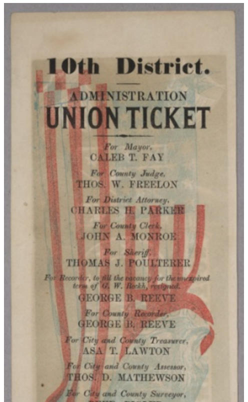
April 18, 2016

Security Goals for an Election

- Integrity: No election fraud

- Transparency: Everyone – especially the loser – must be able to verify that the election was conducted appropriately

- Privacy: No one learns how the voter has voted



10th District.

ADMINISTRATION
UNION TICKET

For Mayor,
CALEB T. FAY

For County Judge,
THOS. W. FREELON

For District Attorney,
CHARLES H. PARKER

For County Clerk,
JOHN A. MONROE

For Sheriff,
THOMAS J. POULTERER

For Recorder, to fill the vacancy for the unexpired term of G. W. Beckh, resigned.
GEORGE B. REEVE

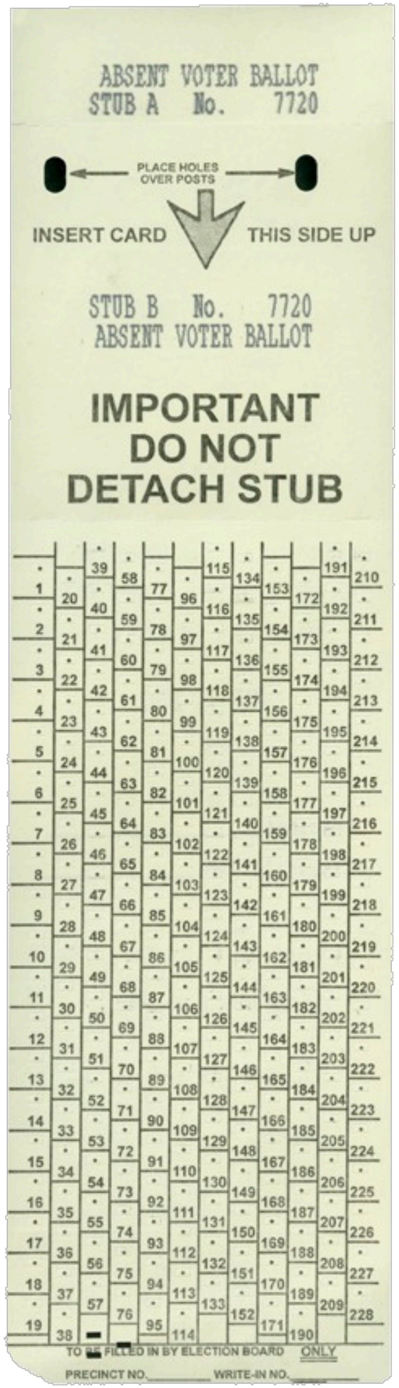
For County Recorder,
GEORGE B. REEVE

For City and County Treasurer,
ASA T. LAWTON

For City and County Assessor,
THOS. D. MATHEWSON

For City and County Surveyor,

- Secret ballot: Voter cannot prove how she voted



ABSENT VOTER BALLOT
STUB A No. 7720

PLACE HOLES OVER POSTS

INSERT CARD THIS SIDE UP

STUB B No. 7720
ABSENT VOTER BALLOT

IMPORTANT
DO NOT
DETACH STUB

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38

39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57

58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76

77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95

96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114

115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133

134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152

153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171

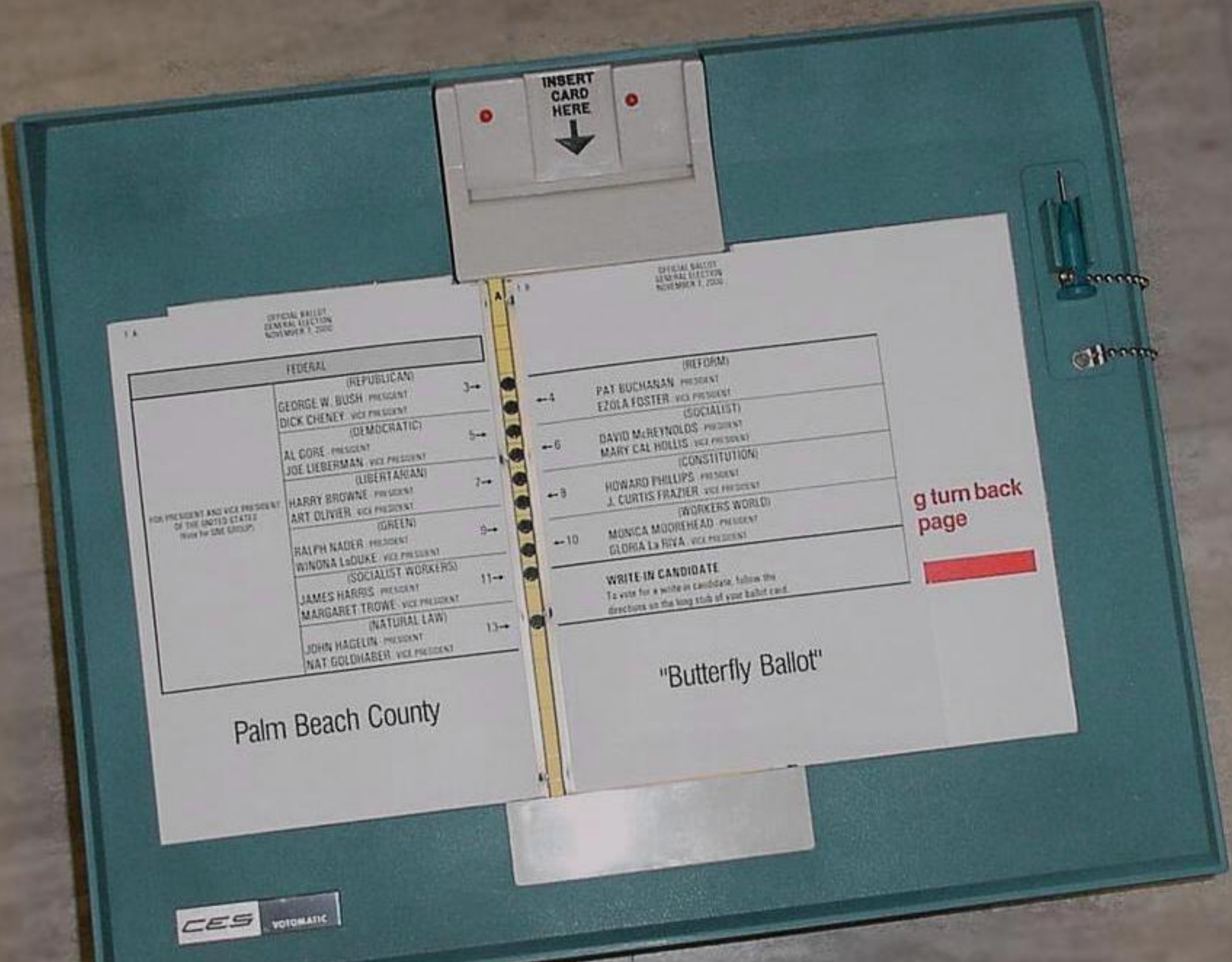
172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190

191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209

210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228

TO BE FILLED IN BY ELECTION BOARD ONLY

PRECINCT NO.________ WRITE-IN NO.________



1 A

OFFICIAL BALLOT
GENERAL ELECTION
NOVEMBER 7, 2000

FEDERAL

FOR PRESIDENT AND VICE PRESIDENT OF THE UNITED STATES (Vote for ONE GROUP)

(REPUBLICAN)
GEORGE W. BUSH PRESIDENT
DICK CHENEY VICE PRESIDENT 3→

(DEMOCRATIC)
AL GORE PRESIDENT
JOE LIEBERMAN VICE PRESIDENT 5→

(LIBERTARIAN)
HARRY BROWNE PRESIDENT
ART OLIVIER VICE PRESIDENT 7→

(GREEN)
RALPH NADER PRESIDENT
WINONA LaDUKE VICE PRESIDENT 9→

(SOCIALIST WORKERS)
JAMES HARRIS PRESIDENT
MARGARET TROWE VICE PRESIDENT 11→

(NATURAL LAW)
JOHN HAGELIN PRESIDENT
NAT GOLDHABER VICE PRESIDENT 13→

1 B

OFFICIAL BALLOT
GENERAL ELECTION
NOVEMBER 7, 2000

(REFORM)
←4 PAT BUCHANAN PRESIDENT
EZOLA FOSTER VICE PRESIDENT

(SOCIALIST)
←6 DAVID McREYNOLDS PRESIDENT
MARY CAL HOLLIS VICE PRESIDENT

(CONSTITUTION)
←8 HOWARD PHILLIPS PRESIDENT
J. CURTIS FRAZIER VICE PRESIDENT

(WORKERS WORLD)
←10 MONICA MOOREHEAD PRESIDENT
GLORIA La RIVA VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

Palm Beach County

"Butterfly Ballot"

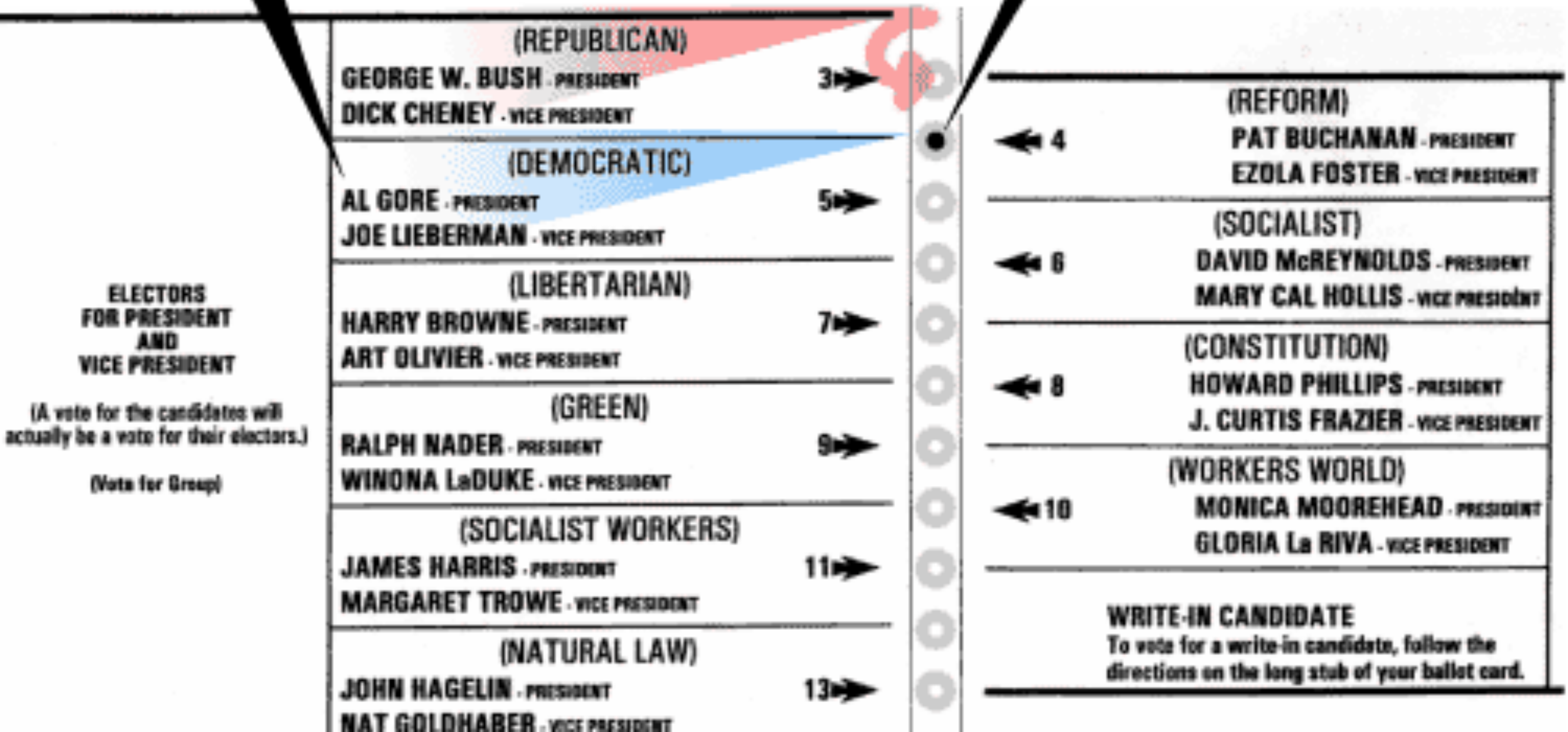
g turn back
page

Confusion at Palm Beach County polls

Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot's design.

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform party.



ELECTORS
FOR PRESIDENT
AND
VICE PRESIDENT

(A vote for the candidates will actually be a vote for their electors.)

(Vote for Group)

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3→

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5→

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7→

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9→

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11→

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13→

←4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

←6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

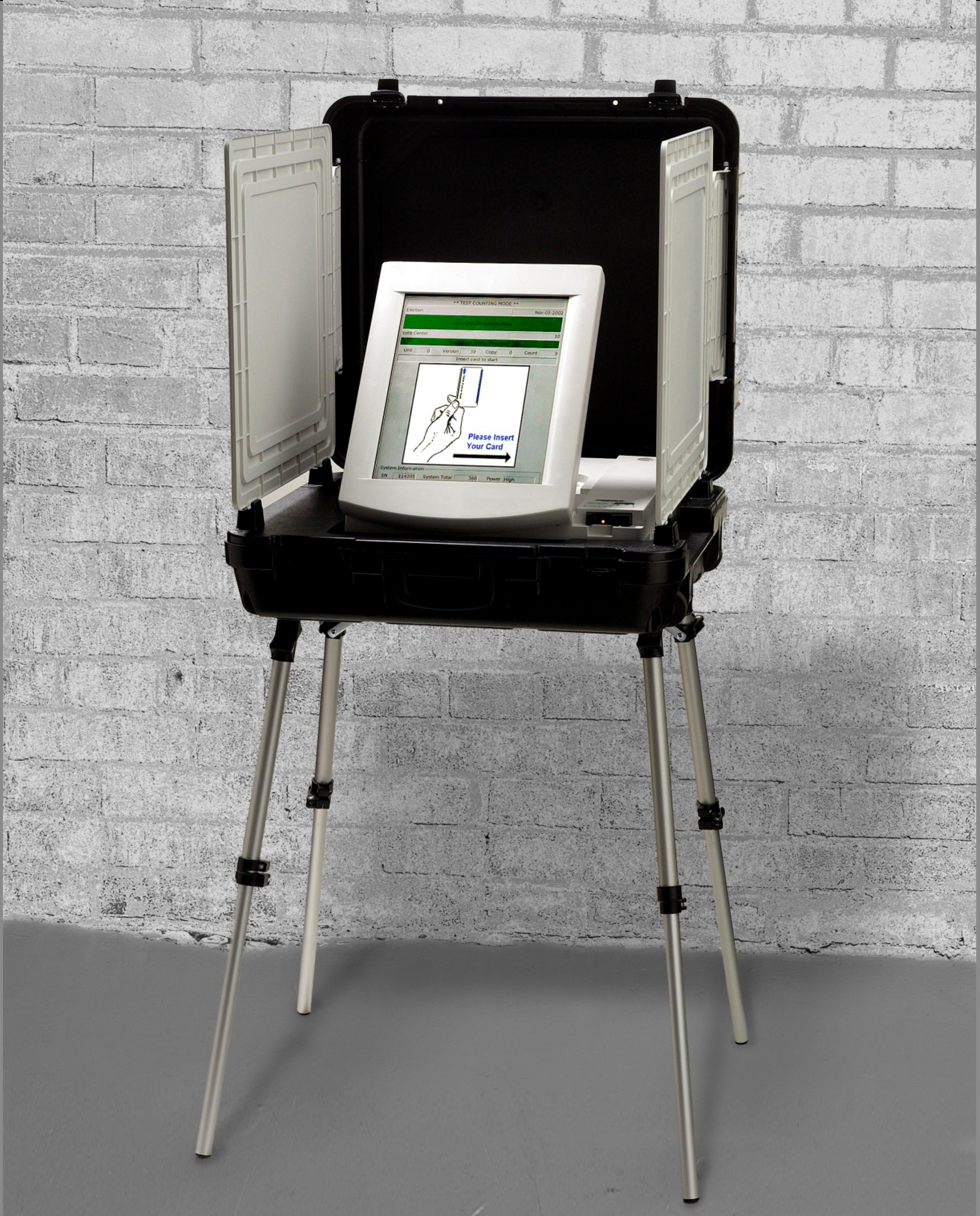
←8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

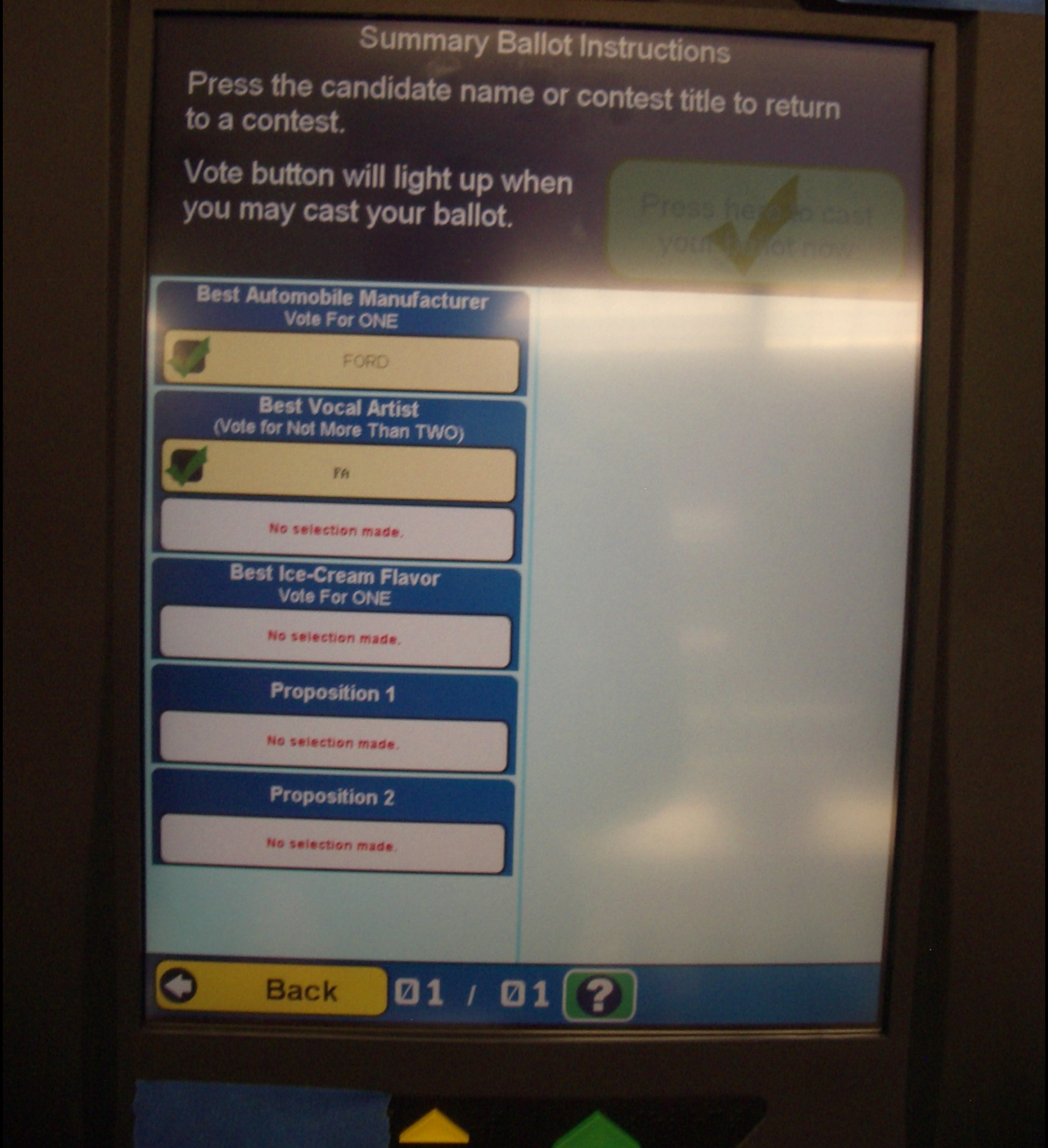
←10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

Another anomaly during the 2000 election

> From: Lana Hires
> Subject: 2000 November Election
>
> I need some answers! Our department is being audited by the County.
>
> I have been waiting for someone to give me an explanation as to why Precinct 216 gave Al Gore a minus 16022 when it was uploaded. Will someone please explain this so that I have the information to give the auditor instead of standing here "looking dumb".


** TEST COUNTING MODE **
Election
Nov-05-2002
Georgia Demonstration
Vote Center
10
Demonstration Precinct
Unit 0
Version 39
Copy 0
Count 9
Insert card to start
Please Insert Your Card
System Information
SN 114995
System Total 366
Power High



Summary Ballot Instructions

Press the candidate name or contest title to return to a contest.

Vote button will light up when you may cast your ballot.

Press here to cast your ballot now.

Best Automobile Manufacturer
Vote For ONE

☑ FORD

Best Vocal Artist
(Vote for Not More Than TWO)

☑ FA

No selection made.

Best Ice-Cream Flavor
Vote For ONE

No selection made.

Proposition 1

No selection made.

Proposition 2

No selection made.

Question: What are the security requirements for electronic voting machines?

1. Machine must allow each authorized voter to vote exactly once; must prevent tampering with votes after they are cast.

2. Machine should be verifiably trustworthy.

3. Machine must randomize the order in which votes were cast.

4. Machine must not give voter a “receipt”.

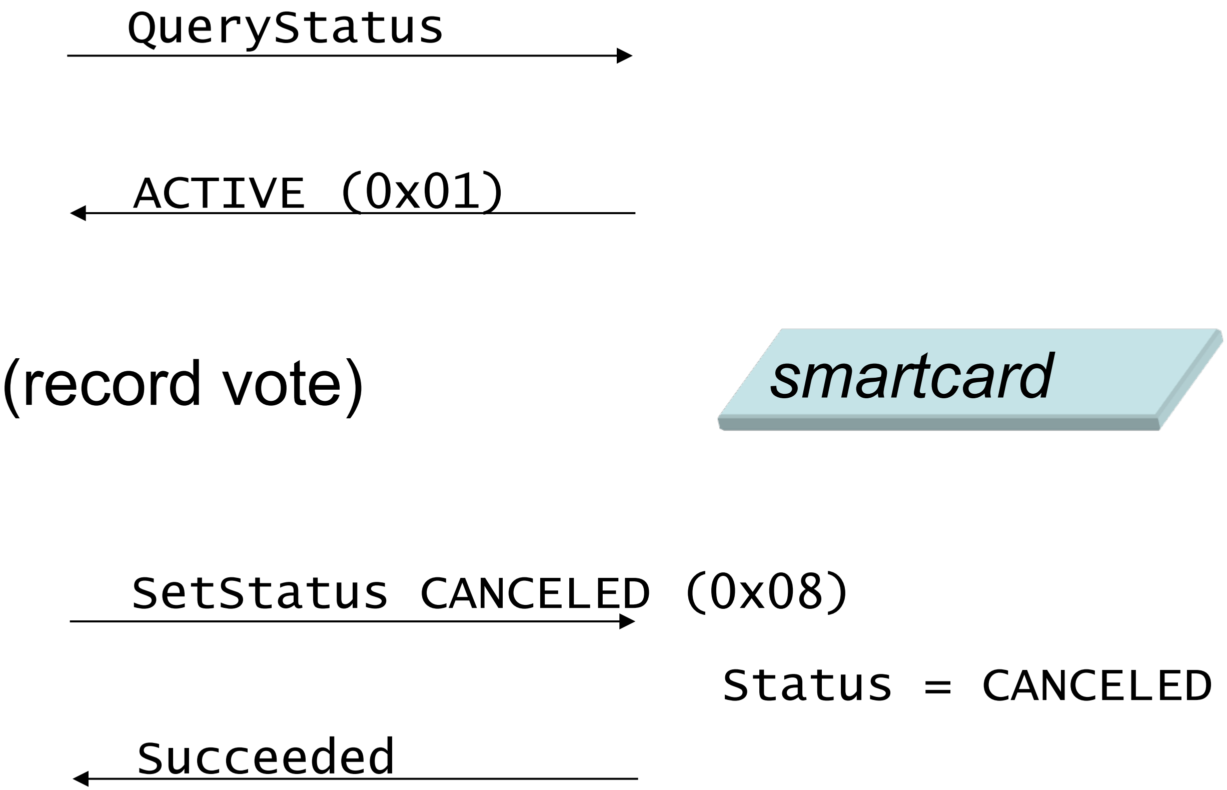
☞ Security goals for an election:
Integrity, Transparency, Privacy, Secret ballot

Nov 4, 2002:
State of Georgia votes on Diebold DREs.

March 18, 2003:
Diebold source code leaks.

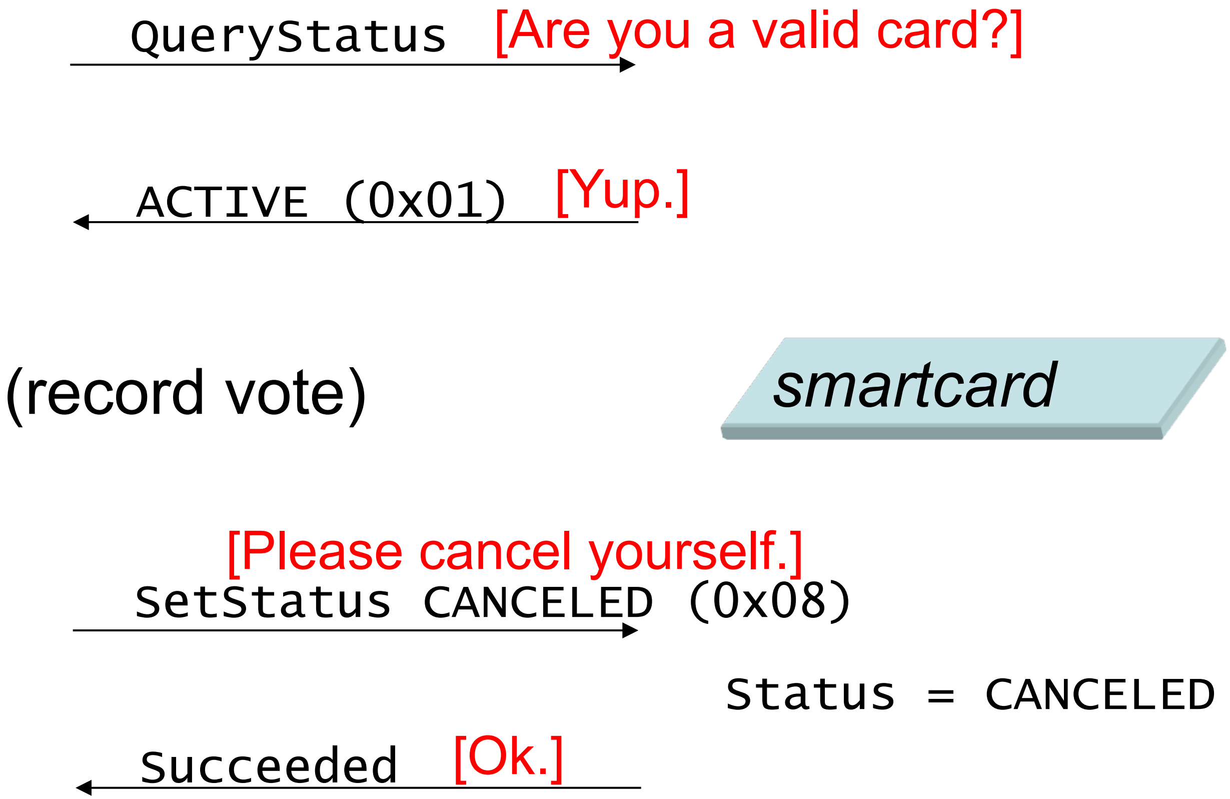
July 23, 2003:
Tadayoshi Kohno, Adam Stubblefield, Avi Rubin, Dan Wallach, “Analysis of an Electronic Voting System”.

The voter authorization protocol



```
QueryStatus →
← ACTIVE (0x01)
(record vote)
smartcard
SetStatus CANCELED (0x08) →
Status = CANCELED
← Succeeded
```

The voter authorization protocol



`QueryStatus` [Are you a valid card?]

`ACTIVE (0x01)` [Yup.]

(record vote)

smartcard

[Please cancel yourself.]

`SetStatus CANCELED (0x08)`

`Status = CANCELED`

`Succeeded` [Ok.]

Attack!

QueryStatus →

← ACTIVE (0x01)

(record vote)

SetStatus CANCELED (0x08) →

← Succeeded

malicious smartcard

QueryStatus →

← ACTIVE (0x01)

(record another vote)

SetStatus CANCELED (0x08) →

← Succeeded

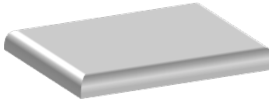
Authenticating election officials

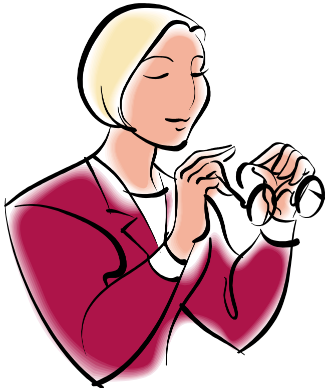
What kind of card are you?

An administrator card.

What's the secret PIN?

2301





What's the secret PIN?

2301

Ok, you have admin access.

Source code excerpts

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

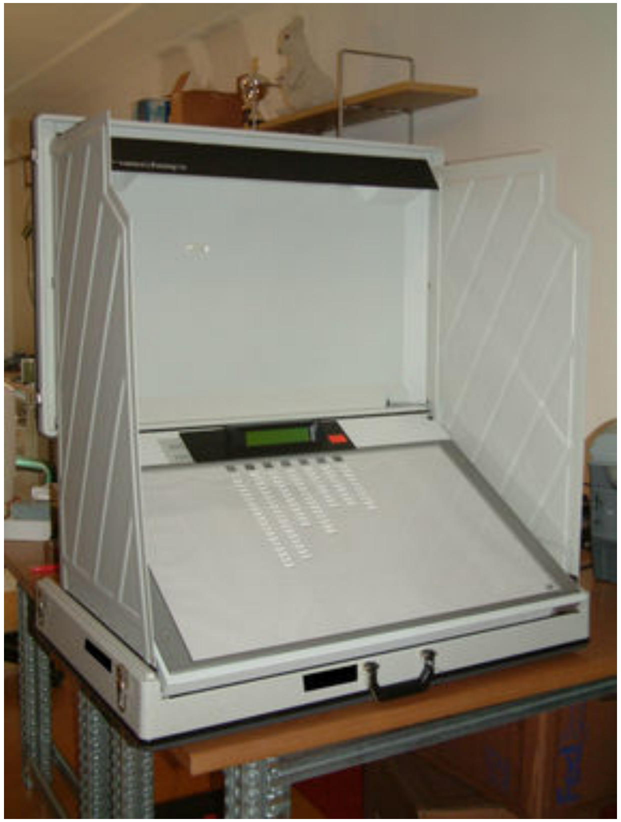
```
DESCBCEncrypt((des_c_block*)tmp,
(des_c_block*)record.m_Data, totalSize,
DESKEY, NULL, DES_ENCRYPT);
```

Source code excerpts

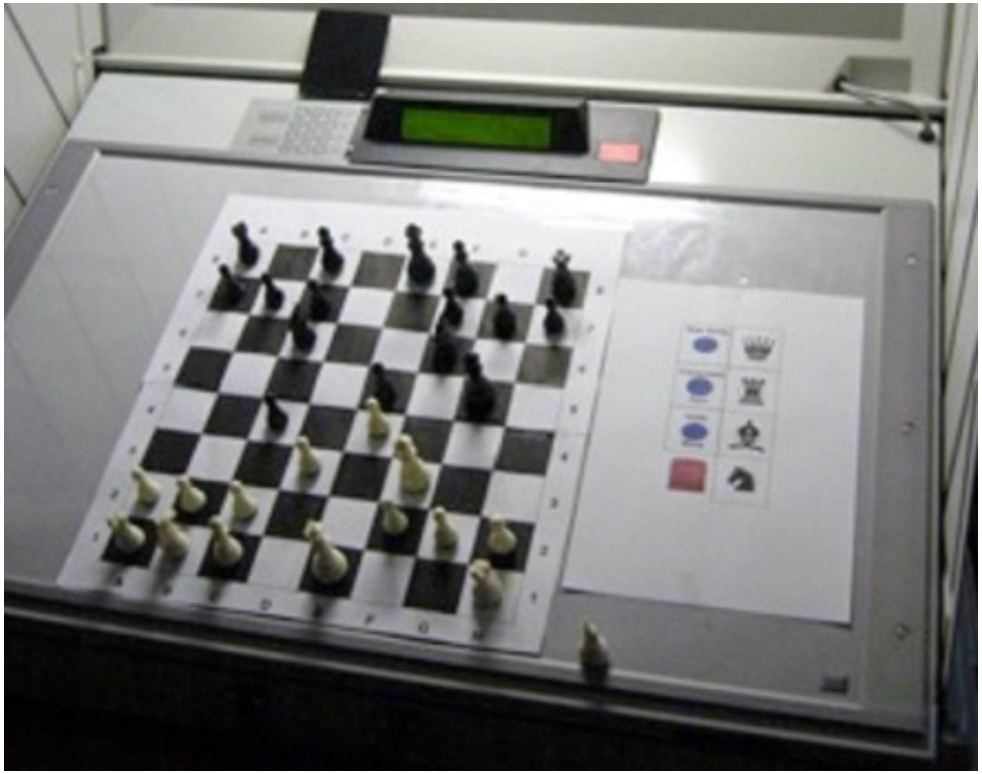
```
// LCG - Linear Congruential Generator -
// used to generate ballot serial numbers
// A psuedo-random-sequence generator
// (per Applied Cryptography, Bruce Schneier)

int lcgGenerator(int lastSN) {
  return ((lastSN*1366) + 150889)%714025;
}
```

"Unfortunately, linear congruential generators cannot be used for cryptography."
— Applied Cryptography, p.369

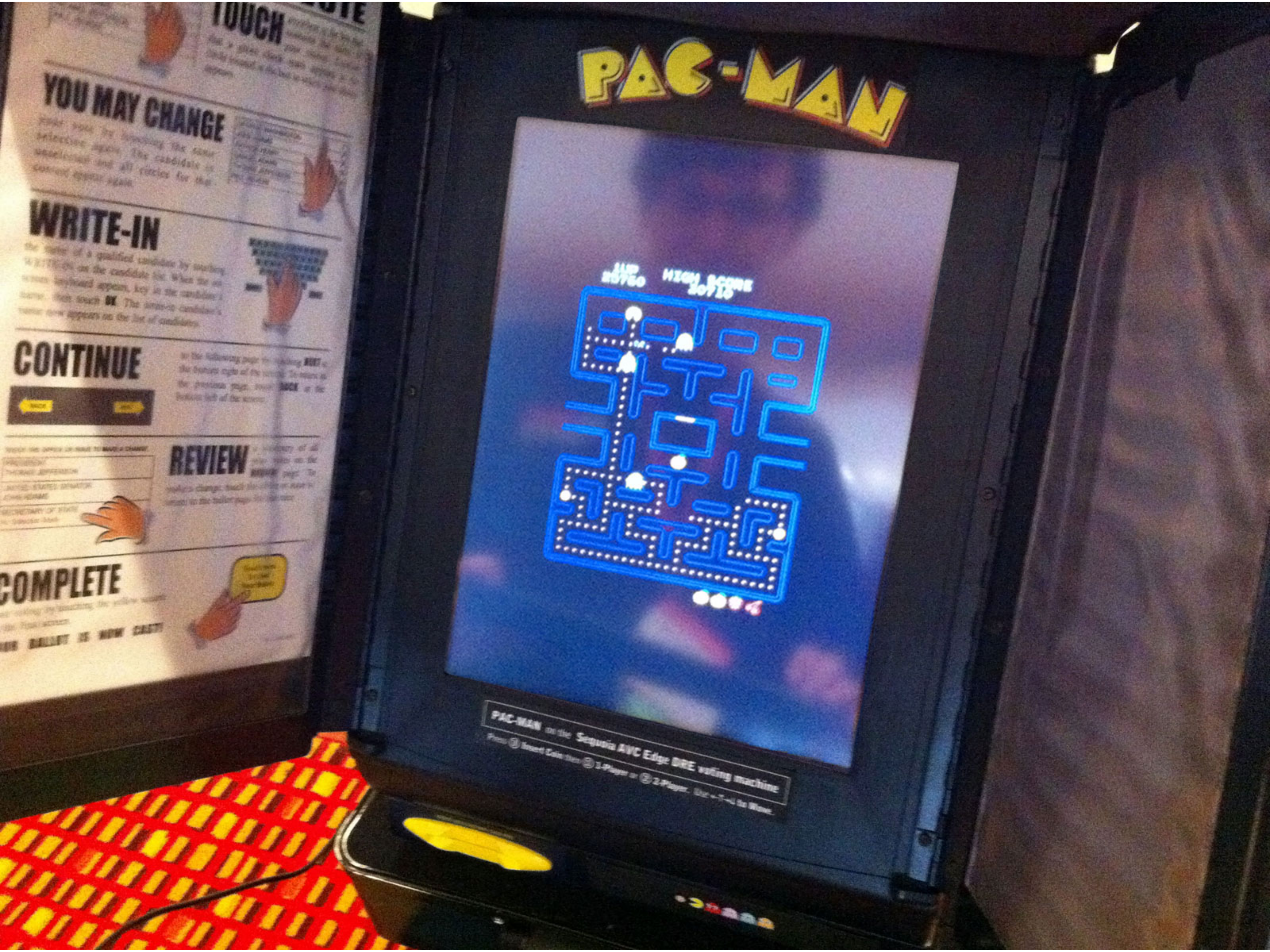
Vendor reactions



`Not a computer,
can't be hacked.'



Yes it can!


TOUCH
YOU MAY CHANGE
WRITE-IN
CONTINUE
REVIEW
COMPLETE
PAC-MAN
1UP
HIGH SCORE
PAC-MAN on the Sequoia AVC Edge DRE voting machine
Press Insert Coin then 1-Player or 2-Player. Use to Move.

More than 4,500 North Carolina votes lost because of mistake in voting machine capacity

JACKSONVILLE, N.C. (AP) — More than 4,500 votes have been lost in one North Carolina county because officials believed a computer that stored ballots electronically could hold more data than it did. Scattered other problems may change results in races around the state.

Officials said UniLect Corp., the maker of the county’s electronic voting system, told them that each storage unit could handle 10,500 votes, but the limit was actually 3,005 votes.

Machine error gives Bush 3,893 extra votes in Ohio

By John McCarthy, Associated Press

COLUMBUS, Ohio — An error with an electronic voting system gave President Bush 3,893 extra votes in suburban Columbus, elections officials said.

Franklin County’s unofficial results had Bush receiving 4,258 votes to Democrat John Kerry’s 260 votes in a precinct in Gahanna. Records show only 638 voters cast ballots in that precinct. Bush’s total should have been recorded as 365.

Fall 2003, Ohio

"I am committed to helping Ohio deliver its electoral votes to the president.”

-- Wally O’Dell

CEO of Diebold

http://denvervoice.org
-MAR

LIVE FREE DIEBOLD
ELECTRONIC VOTING IS UNRELIABLE
PAPER BALLOTS 2004
THE COMPUTER ATE MY VOTE!

VOTING WITHOUT AUDITING ARE WE INSANE?
SECRET SOFT WARE SECRET GOVERNMENT

HOW LONG WILL It TAKE TO GET It RIGHT

ELECTION FRAUD
MEDIA BLACKOUT

VOTE BUT VERIFY!

NO MORE WAR
Live Free Die Bold
LIVE FREE or DIE BOLD
BE THE CHANGE
VISUALIZE TRUE DEMOCRACY
VISUALIZE LEGITIMATE, SECURE ELECTIONS
Paper Ballots Hand Counted

California Top-to-Bottom Review

In 2007, California Secretary of State Debra Bowen commissions a review of California's voting systems.

43 experts (led by David Wagner & Matt Bishop) examine voting systems used nationally.

THE SECRETARY
Bowen opens the public hearing in Sacramento.

Technical findings of the CA TTBR

All voting systems examined have serious security problems:

- None followed sound engineering principles expected of security-critical systems.
- All were vulnerable to viral attacks: one outsider could subvert all voting machines countywide

Example flaw (Diebold/Premier system)

Bug: The code that reads data off the memory card has buffer overrun vulnerabilities.

Attack:

1. Attacker writes malicious code onto 1 card
2. When central PC reads votes off card on election night, it gets infected
3. Infected PC writes malicious code onto all cards used in the next election, infecting entire county

Quotes from the reports

“We found pervasive security weaknesses throughout the Sequoia software. Virtually every important software security mechanism is vulnerable to circumvention.”

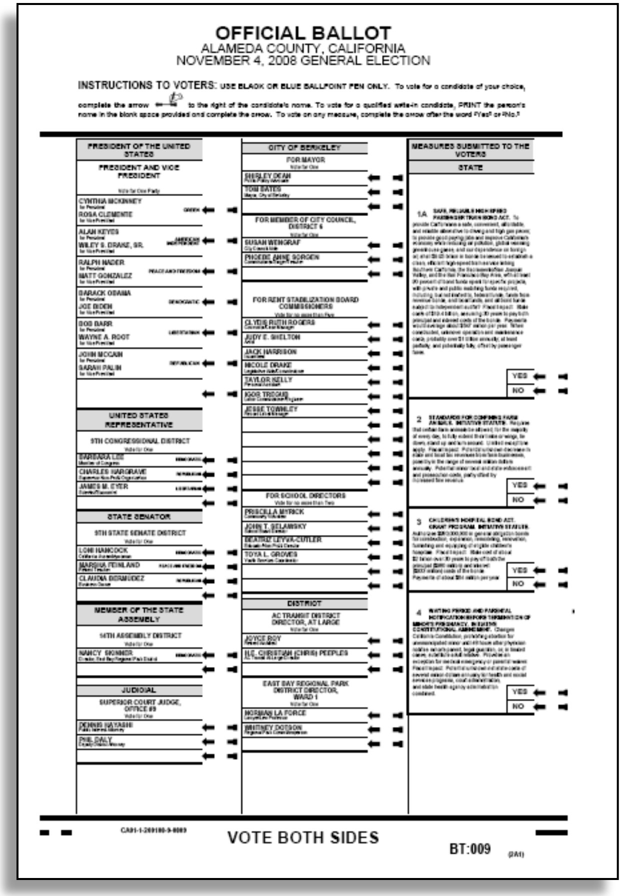
“Our study of the Diebold source code found that the system does not meet the requirements for a security-critical system. It is built upon an inherently fragile design and suffers from implementation flaws that can expose the entire voting system to attacks.”

“The Hart software and devices appear to be susceptible to a variety of attacks which would allow an attacker to gain control of some or all of the systems in a county. [..] Many of these attacks can be mounted in a manner that makes them extremely hard to detect and correct. We expect that many of them could be carried out in the field by a single individual, without extensive effort, and without long-term access to the equipment.”

Outcome of the CA TTBR

Bowen decertifies most touchscreen e-voting machines and imposes strict new procedural protections.

Result: Most Californians now vote on paper ballots.



OFFICIAL BALLOT
ALAMEDA COUNTY, CALIFORNIA
NOVEMBER 4, 2008 GENERAL ELECTION

INSTRUCTIONS TO VOTERS: USE BLACK OR BLUE BALLPOINT PEN ONLY. To vote for a candidate of your choice, complete the arrow to the right of the candidate's name. To vote for a qualified write-in candidate, PRINT the person's name in the blank space provided and complete the arrow. To vote on any measure, complete the arrow after the word "Yes" or "No."

PRESIDENT OF THE UNITED STATES

PRESIDENT AND VICE PRESIDENT
Vote for One Party

CYNTHIA MCKINNEY for President
ROSA CLEMENTE for Vice President — GREEN

ALAN KEYES for President
WILEY S. DRAKE, SR. for Vice President — AMERICAN INDEPENDENT

RALPH NADER for President
MATT GONZALEZ for Vice President — PEACE AND FREEDOM

BARACK OBAMA for President
JOE BIDEN for Vice President — DEMOCRATIC

BOB BARR for President
WAYNE A. ROOT for Vice President — LIBERTARIAN

JOHN MCCAIN for President
SARAH PALIN for Vice President — REPUBLICAN

UNITED STATES REPRESENTATIVE

9TH CONGRESSIONAL DISTRICT
Vote for One

BARBARA LEE Member of Congress — DEMOCRATIC
CHARLES HARGRAVE — REPUBLICAN
JAMES M. EYER — LIBERTARIAN

STATE SENATOR

9TH STATE SENATE DISTRICT
Vote for One

LONI HANCOCK California Assemblywoman — DEMOCRATIC
MARSHA FEINLAND Retired Teacher — PEACE AND FREEDOM
CLAUDIA BERMÚDEZ Business Owner — REPUBLICAN

MEMBER OF THE STATE ASSEMBLY

14TH ASSEMBLY DISTRICT
Vote for One

NANCY SKINNER Director, East Bay Regional Park District — DEMOCRATIC

JUDICIAL

SUPERIOR COURT JUDGE, OFFICE #9
Vote for One

DENNIS HAYASHI Public Interest Attorney
PHIL DALY Deputy District Attorney

CITY OF BERKELEY

FOR MAYOR
Vote for One

SHIRLEY DEAN Public Policy Advocate
TOM BATES Mayor, City of Berkeley

FOR MEMBER OF CITY COUNCIL, DISTRICT 6
Vote for One

SUSAN WENGRAF City Council Aide
PHOEBE ANNE SORGEN

FOR RENT STABILIZATION BOARD COMMISSIONERS
Vote for no more than Five

CLYDIS RUTH ROGERS
JUDY E. SHELTON Artist
JACK HARRISON
NICOLE DRAKE Legislative Aide/Coordinator
TAYLOR KELLY
IGOR TREGUB
JESSE TOWNLEY

FOR SCHOOL DIRECTORS
Vote for no more than Two

PRISCILLA MYRICK Community Volunteer
JOHN T. SELAWSKY School Board Director
BEATRIZ LEYVA-CUTLER Educator/Non-Profit Director
TOYA L. GROVES Youth Services Coordinator

DISTRICT

AC TRANSIT DISTRICT DIRECTOR, AT LARGE
Vote for One

JOYCE ROY
H.E. CHRISTIAN (CHRIS) PEEPLES AC Transit At-Large Director

EAST BAY REGIONAL PARK DISTRICT DIRECTOR, WARD 1
Vote for One

NORMAN LA FORCE
WHITNEY DOTSON

MEASURES SUBMITTED TO THE VOTERS

STATE

1A SAFE, RELIABLE HIGH-SPEED PASSENGER TRAIN BOND ACT. To provide Californians a safe, convenient, affordable, and reliable alternative to driving and high gas prices; to provide good-paying jobs and improve California's economy while reducing air pollution, global warming greenhouse gases, and our dependence on foreign oil, shall $9.95 billion in bonds be issued to establish a clean, efficient high-speed train service linking Southern California, the Sacramento/San Joaquin Valley, and the San Francisco Bay Area, with at least 90 percent of bond funds spent for specific projects, with private and public matching funds required, including, but not limited to, federal funds, funds from revenue bonds, and local funds, and all bond funds subject to independent audits? Fiscal Impact: State costs of $19.4 billion, assuming 30 years to pay both principal and interest costs of the bonds. Payments would average about $647 million per year. When constructed, unknown operation and maintenance costs, probably over $1 billion annually; at least partially, and potentially fully, offset by passenger fares.

YES
NO

2 STANDARDS FOR CONFINING FARM ANIMALS. INITIATIVE STATUTE. Requires that certain farm animals be allowed, for the majority of every day, to fully extend their limbs or wings, lie down, stand up and turn around. Limited exceptions apply. Fiscal Impact: Potential unknown decrease in state and local tax revenues from farm businesses, possibly in the range of several million dollars annually. Potential minor local and state enforcement and prosecution costs, partly offset by increased fine revenue.

YES
NO

3 CHILDREN'S HOSPITAL BOND ACT. GRANT PROGRAM. INITIATIVE STATUTE. Authorizes $980,000,000 in general obligation bonds for construction, expansion, remodeling, renovation, furnishing and equipping of eligible children's hospitals. Fiscal Impact: State cost of about $2 billion over 30 years to pay off both the principal ($980 million) and interest ($987 million) costs of the bonds. Payments of about $64 million per year.

YES
NO

4 WAITING PERIOD AND PARENTAL NOTIFICATION BEFORE TERMINATION OF MINOR'S PREGNANCY. INITIATIVE CONSTITUTIONAL AMENDMENT. Changes California Constitution, prohibiting abortion for unemancipated minor until 48 hours after physician notifies minor's parent, legal guardian, or, in limited cases, substitute adult relative. Provides an exception for medical emergency or parental waiver. Fiscal Impact: Potential unknown net state costs of several million dollars annually for health and social services programs, court administration, and state health agency administration combined.

YES
NO

CA01-1-200100-9-0009

VOTE BOTH SIDES

BT:009 (2A1)

Trojan Horses and the Insider Threat

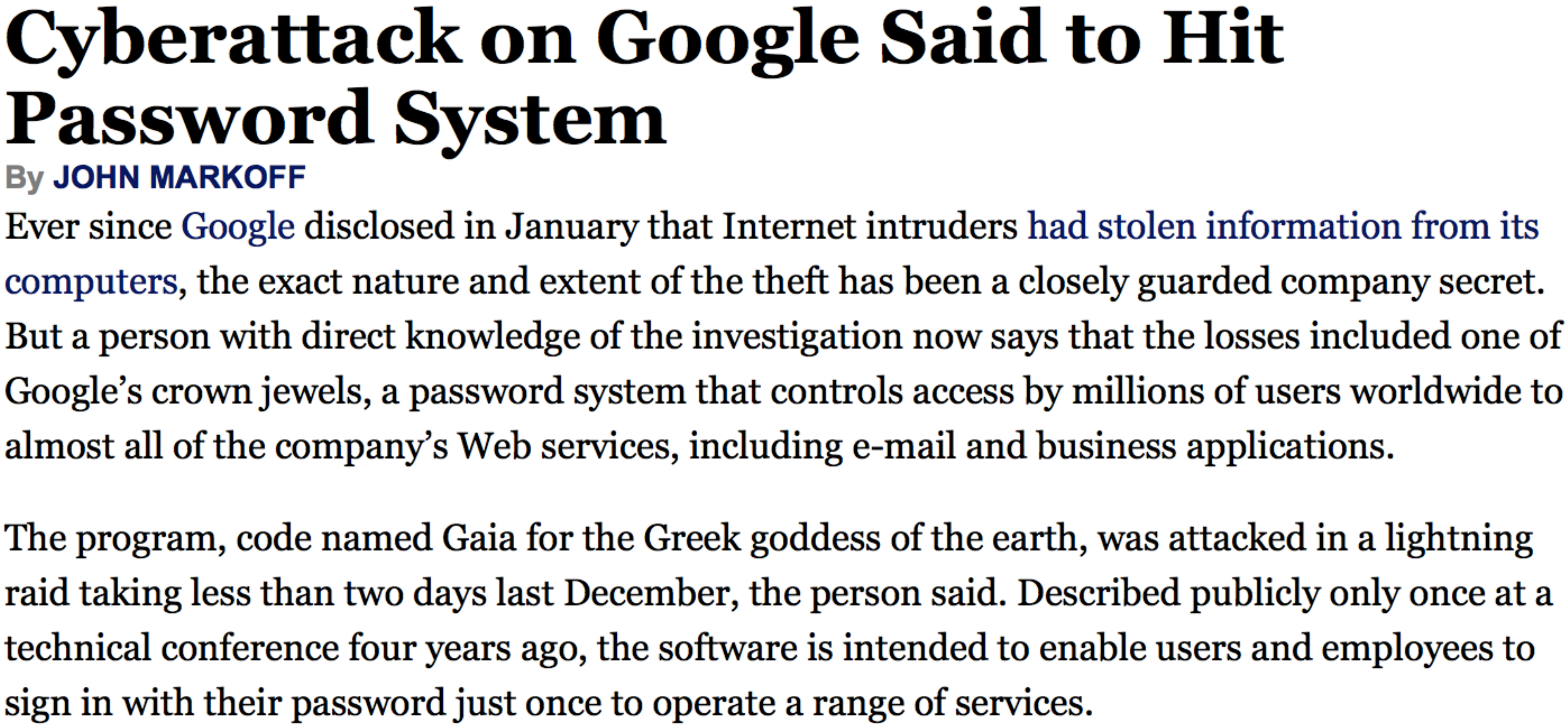
Ronald Dale Harris

Employee, Gaming Control Board, 1983-1995

Arrested, Jan 15,1995
Convicted, Sept 23, 1997, for rigging slot machines

Attempted Trojan Horse in Linux Kernel

```
        …
        schedule();
        goto repeat;
}
if ((options == (__WCLONE|__WALL)) && current->uid = 0))
        retval = -EINVAL;
retval = -ECHILD;
end_wait4:
current->state = TASK_RUNNING;
…
```



Cyberattack on Google Said to Hit Password System

By JOHN MARKOFF

Ever since Google disclosed in January that Internet intruders had stolen information from its computers, the exact nature and extent of the theft has been a closely guarded company secret. But a person with direct knowledge of the investigation now says that the losses included one of Google's crown jewels, a password system that controls access by millions of users worldwide to almost all of the company's Web services, including e-mail and business applications.

The program, code named Gaia for the Greek goddess of the earth, was attacked in a lightning raid taking less than two days last December, the person said. Described publicly only once at a technical conference four years ago, the software is intended to enable users and employees to sign in with their password just once to operate a range of services.

Trojan Horses and Voting Machines

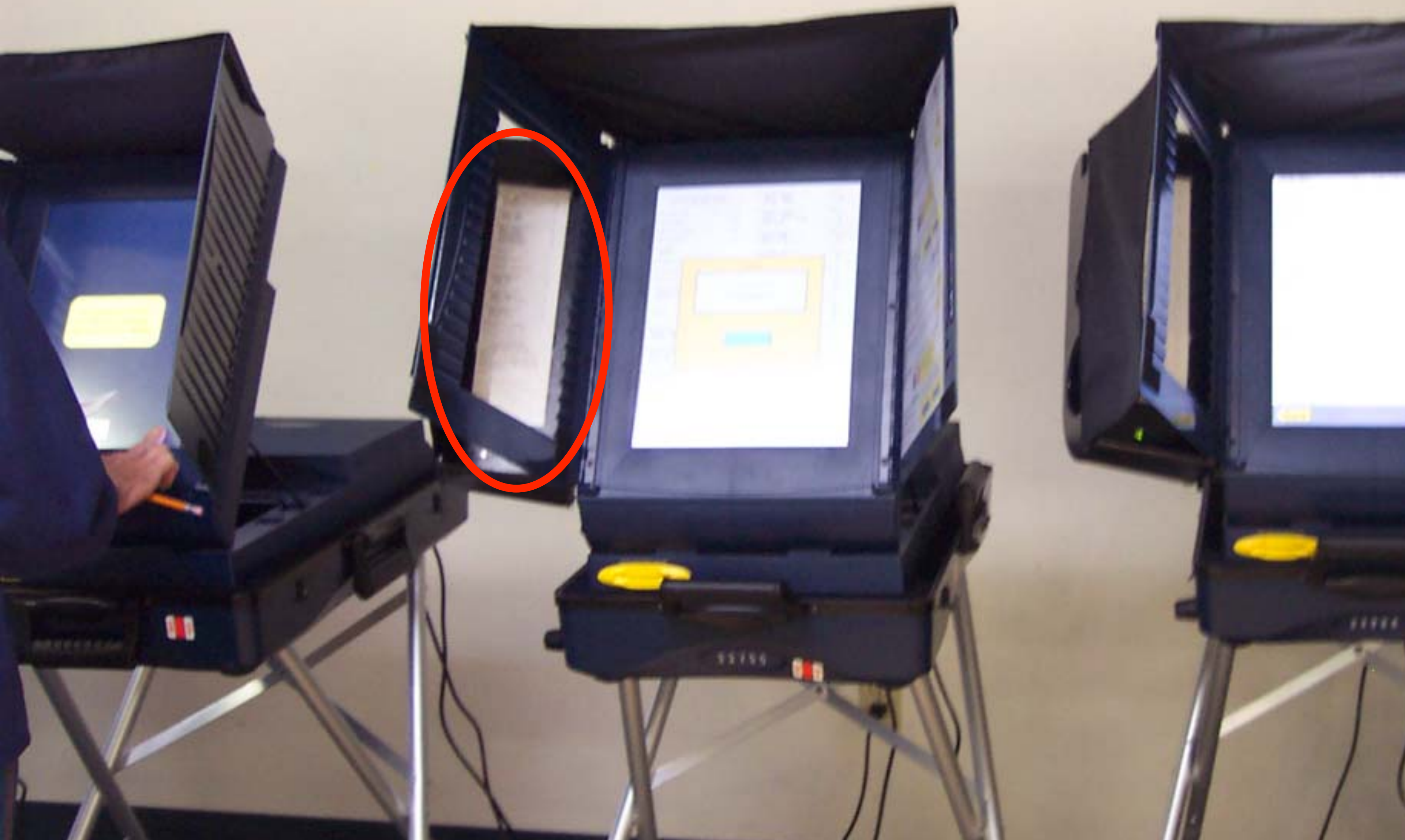
Malicious logic hidden by an insider might, e.g., record votes incorrectly to favor one candidate. How would we defend a voting system against this kind of insider threat?

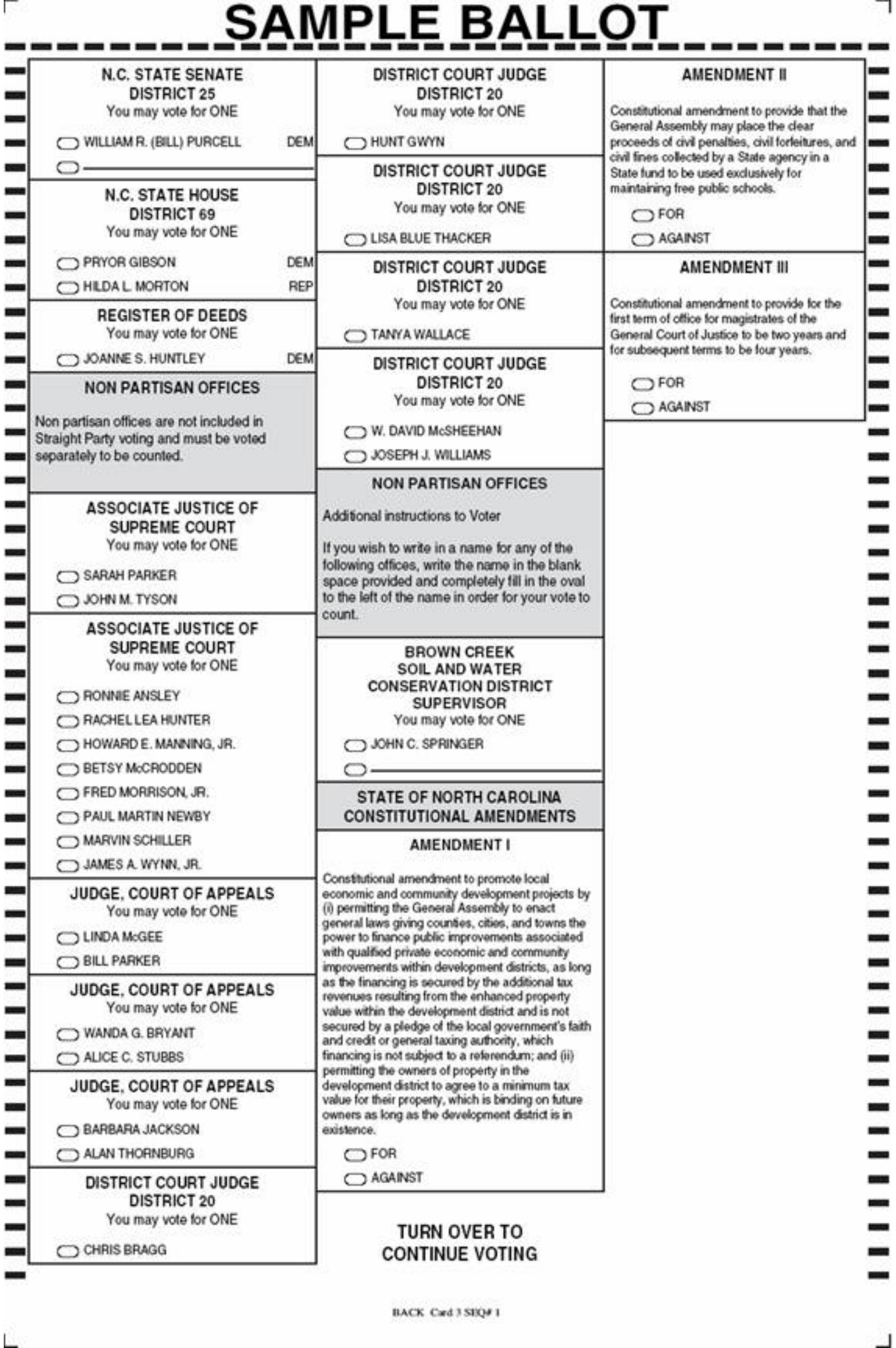
Potential solutions:

- Verify that the software is free of Trojans and will work correctly on all future elections. (beyond the state of the art)

Voting on Satan's computer.

- Assume sw might contain Trojans. Verify that sw worked correctly in this particular election. (voter-verified paper records + random audits)





SAMPLE BALLOT

N.C. STATE SENATE
DISTRICT 25
You may vote for ONE

○ WILLIAM R. (BILL) PURCELL DEM
○ ______

N.C. STATE HOUSE
DISTRICT 69
You may vote for ONE

○ PRYOR GIBSON DEM
○ HILDA L. MORTON REP

REGISTER OF DEEDS
You may vote for ONE

○ JOANNE S. HUNTLEY DEM

NON PARTISAN OFFICES

Non partisan offices are not included in Straight Party voting and must be voted separately to be counted.

ASSOCIATE JUSTICE OF SUPREME COURT
You may vote for ONE

○ SARAH PARKER
○ JOHN M. TYSON

ASSOCIATE JUSTICE OF SUPREME COURT
You may vote for ONE

○ RONNIE ANSLEY
○ RACHEL LEA HUNTER
○ HOWARD E. MANNING, JR.
○ BETSY McCRODDEN
○ FRED MORRISON, JR.
○ PAUL MARTIN NEWBY
○ MARVIN SCHILLER
○ JAMES A. WYNN, JR.

JUDGE, COURT OF APPEALS
You may vote for ONE

○ LINDA McGEE
○ BILL PARKER

JUDGE, COURT OF APPEALS
You may vote for ONE

○ WANDA G. BRYANT
○ ALICE C. STUBBS

JUDGE, COURT OF APPEALS
You may vote for ONE

○ BARBARA JACKSON
○ ALAN THORNBURG

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE

○ CHRIS BRAGG

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE

○ HUNT GWYN

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE

○ LISA BLUE THACKER

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE

○ TANYA WALLACE

DISTRICT COURT JUDGE
DISTRICT 20
You may vote for ONE

○ W. DAVID McSHEEHAN
○ JOSEPH J. WILLIAMS

NON PARTISAN OFFICES

Additional instructions to Voter

If you wish to write in a name for any of the following offices, write the name in the blank space provided and completely fill in the oval to the left of the name in order for your vote to count.

BROWN CREEK
SOIL AND WATER
CONSERVATION DISTRICT
SUPERVISOR
You may vote for ONE

○ JOHN C. SPRINGER
○ ______

STATE OF NORTH CAROLINA
CONSTITUTIONAL AMENDMENTS

AMENDMENT I

Constitutional amendment to promote local economic and community development projects by (i) permitting the General Assembly to enact general laws giving counties, cities, and towns the power to finance public improvements associated with qualified private economic and community improvements within development districts, as long as the financing is secured by the additional tax revenues resulting from the enhanced property value within the development district and is not secured by a pledge of the local government's faith and credit or general taxing authority, which financing is not subject to a referendum; and (ii) permitting the owners of property in the development district to agree to a minimum tax value for their property, which is binding on future owners as long as the development district is in existence.

○ FOR
○ AGAINST

TURN OVER TO
CONTINUE VOTING

AMENDMENT II

Constitutional amendment to provide that the General Assembly may place the clear proceeds of civil penalties, civil forfeitures, and civil fines collected by a State agency in a State fund to be used exclusively for maintaining free public schools.

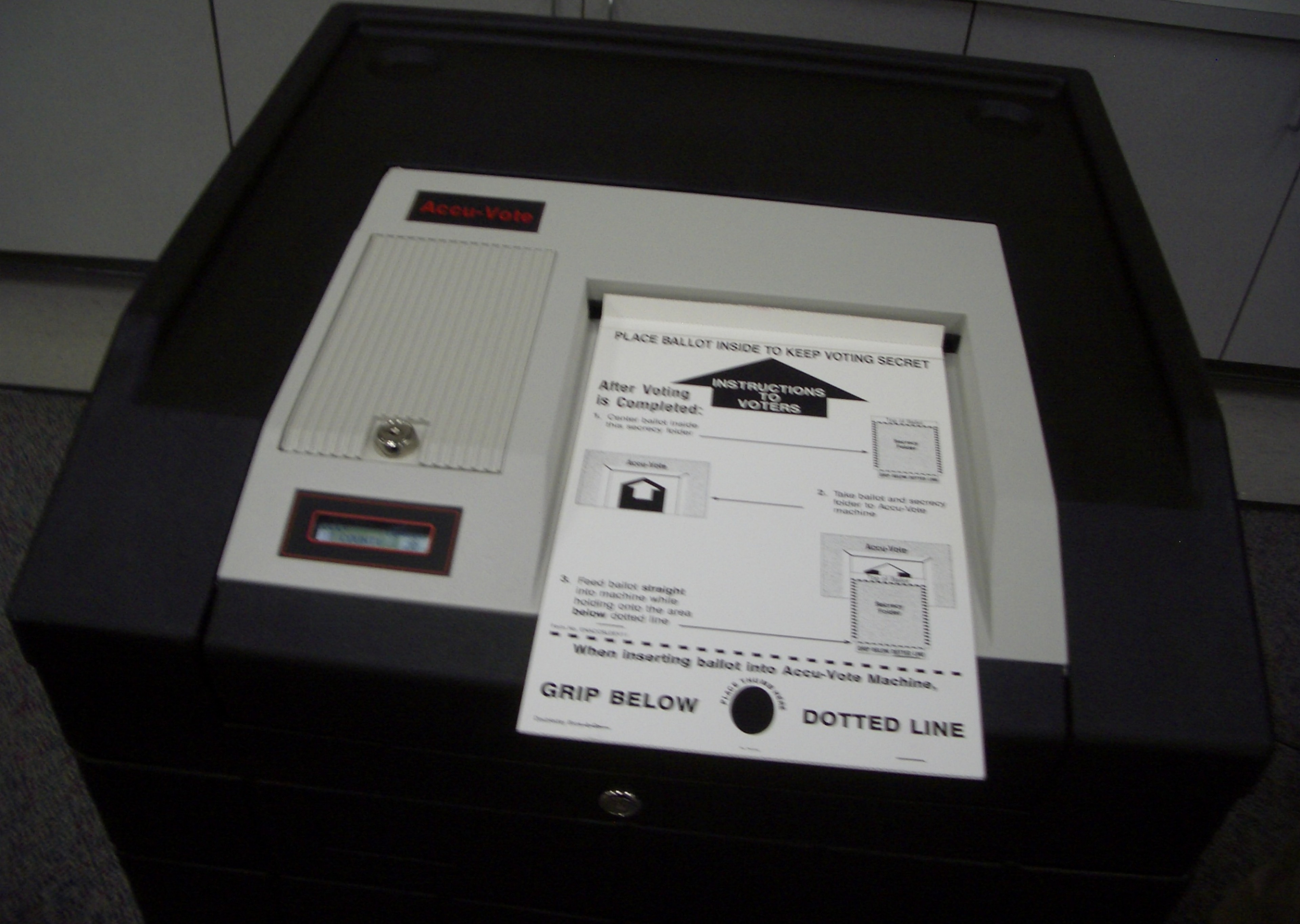
○ FOR
○ AGAINST

AMENDMENT III

Constitutional amendment to provide for the first term of office for magistrates of the General Court of Justice to be two years and for subsequent terms to be four years.

○ FOR
○ AGAINST

BACK Card 3 SEQ# 1



PLACE BALLOT INSIDE TO KEEP VOTING SECRET

INSTRUCTIONS TO VOTERS

After Voting is Completed:

1. Center ballot inside this secrecy folder

2. Take ballot and secrecy folder to Accu-Vote machine.

3. Feed ballot **straight** into machine while holding onto the area **below** dotted line

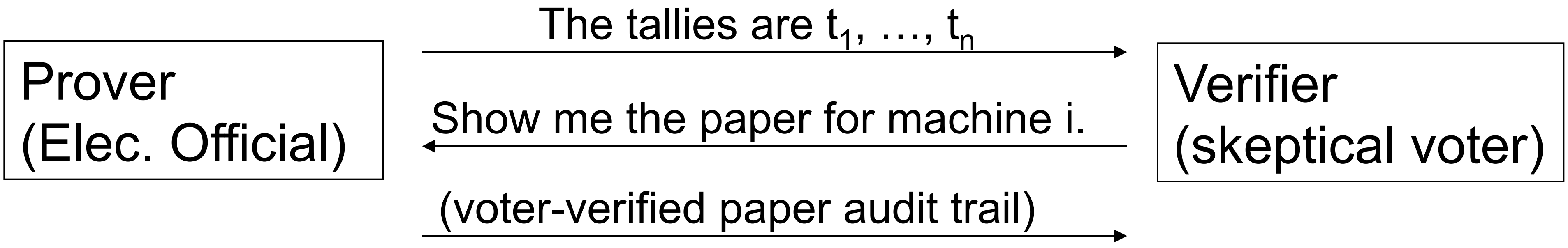
When inserting ballot into Accu-Vote Machine,

GRIP BELOW DOTTED LINE

Statistical audit

- After election, randomly choose 1% of machines and manually recount the paper records on those machines. If paper count ≠ electronic count, there was fraud.

- If » 100 machines cheat, detection is likely. Consequently: If paper count = electronic count, then no more than ~100 machines cheated.



Prover
(Elec. Official)

The tallies are $t_1, \ldots, t_n$

Show me the paper for machine i.

(voter-verified paper audit trail)

Verifier
(skeptical voter)

Conclusions

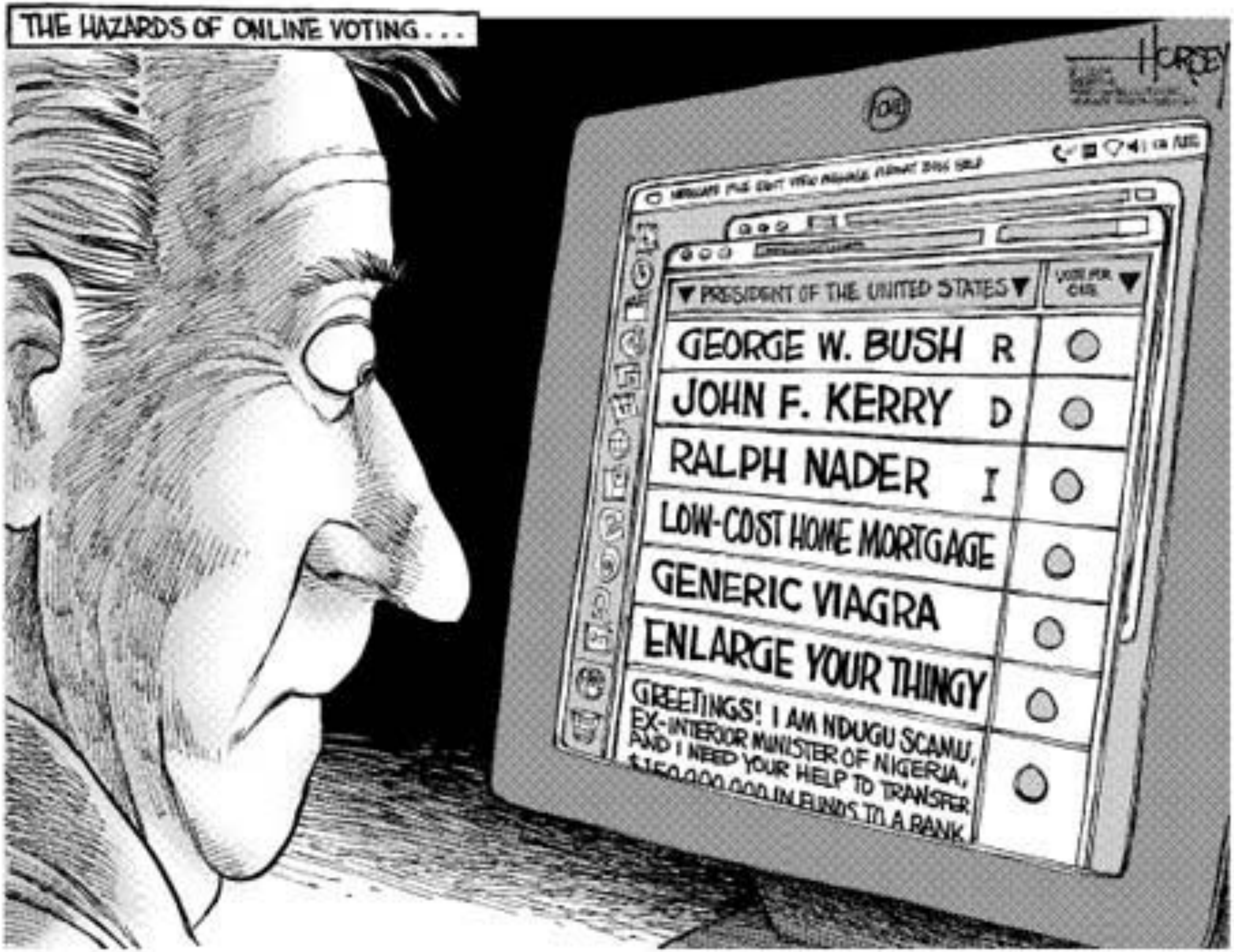
- E-voting security is hard, but...
- E-voting can be made secure and trustworthy, if it can be audited.

- Technical principles:
  - Two-person control, separation of duties
  - Statistical audit
  - Security against malicious insiders

Lessons

- Understand security requirements before you design & deploy an information system.
- Independent review is valuable.
- Sometimes technical threats can be handled through non-technical defenses.
- Seek independent, end-to-end checks that the system is working properly.
- Securing systems against malicious insiders is extremely challenging.
- Business structure determines the technology that is built & deployed. If buyers cannot measure how secure a product is, be prepared for market failures.

Extra Material

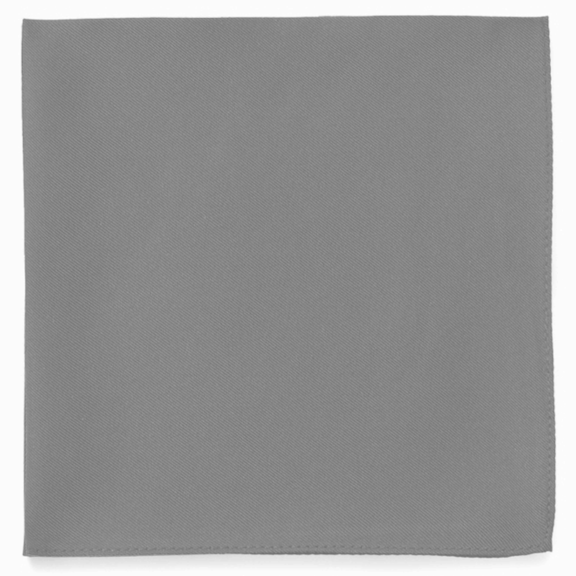

THE HAZARDS OF ONLINE VOTING....
HORSEY
PRESIDENT OF THE UNITED STATES
VOTE FOR ONE
GEORGE W. BUSH R
JOHN F. KERRY D
RALPH NADER I
LOW-COST HOME MORTGAGE
GENERIC VIAGRA
ENLARGE YOUR THINGY
GREETINGS! I AM NDUGU SCAMU, EX-INTERIOR MINISTER OF NIGERIA, AND I NEED YOUR HELP TO TRANSFER $150,000,000 IN FUNDS TO A BANK

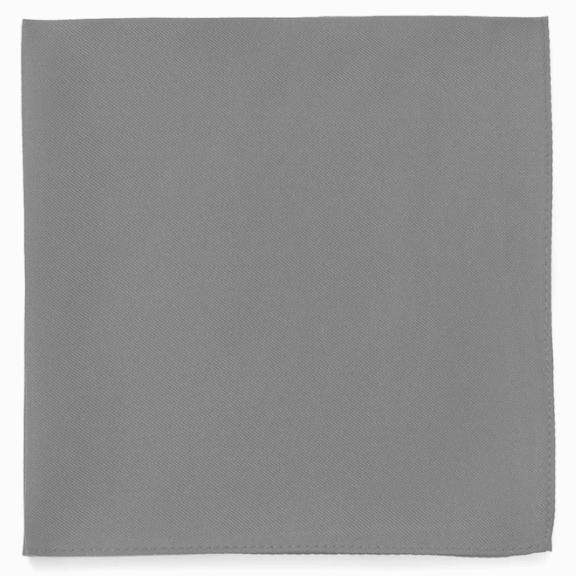
Can I get a volunteer?

Interactive proofs

Here are two cloths.

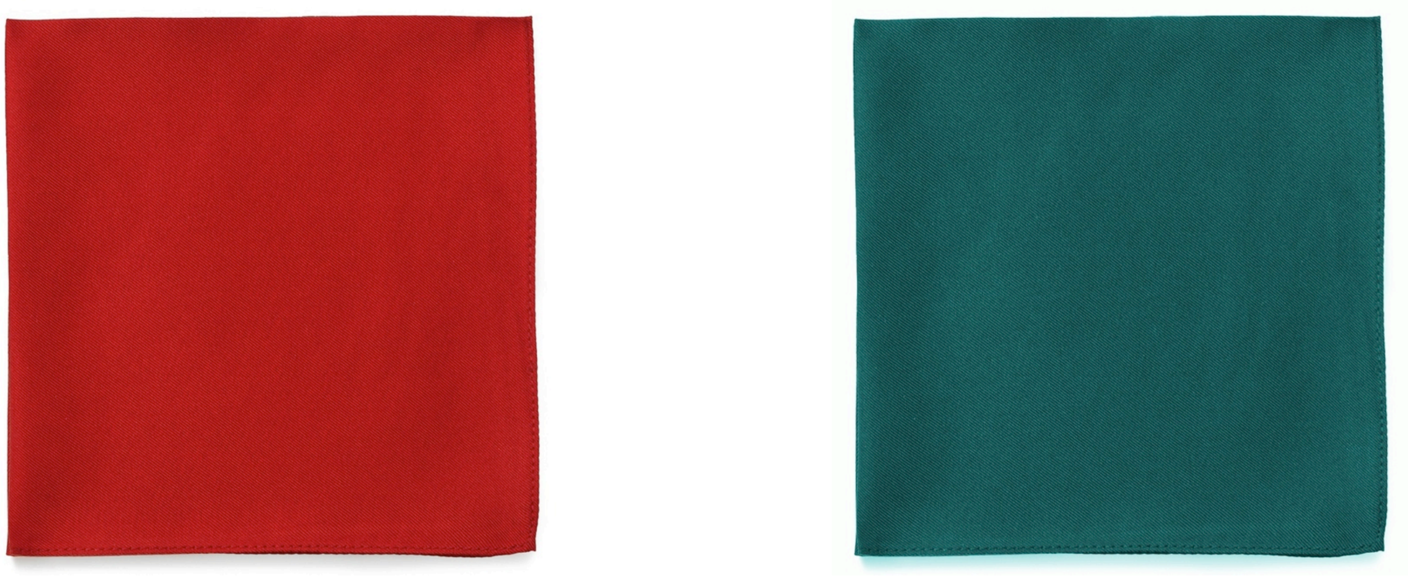
Interactive proofs





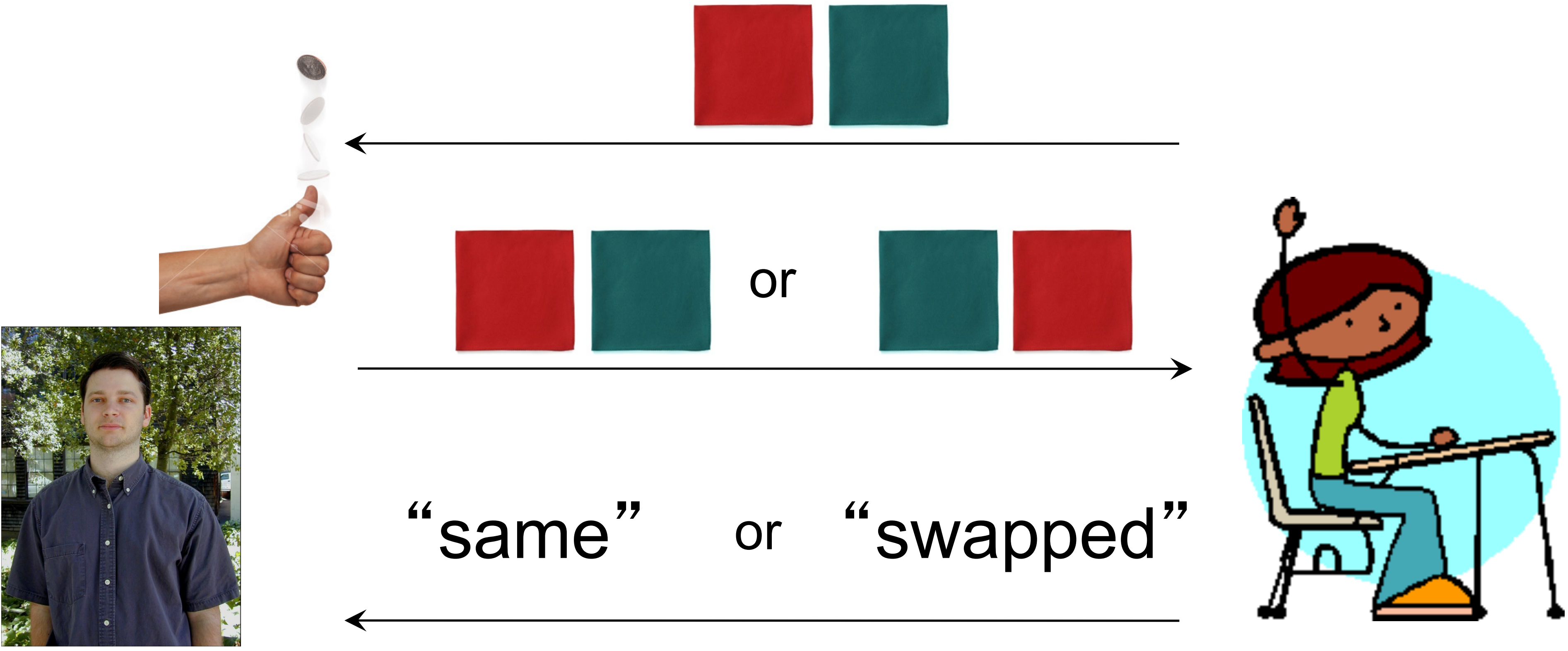
Imagine that I am red-green color-blind…

Interactive proofs



How could you prove to me that you can distinguish the red cloth from the green cloth, if I am red-green color-blind?

An interactive proof



or

“same” or “swapped”

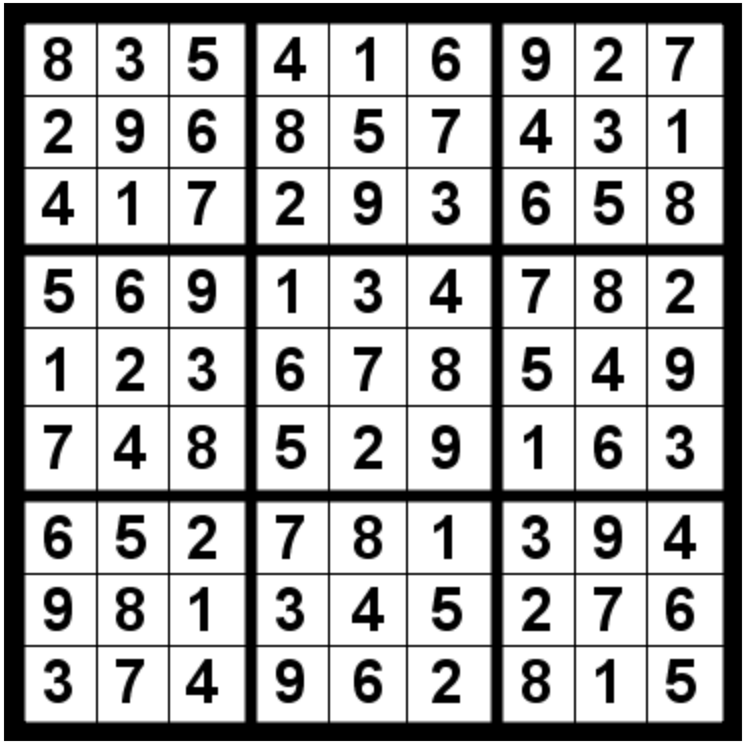
Verifier

Prover

Sudoku

8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

Sudoku

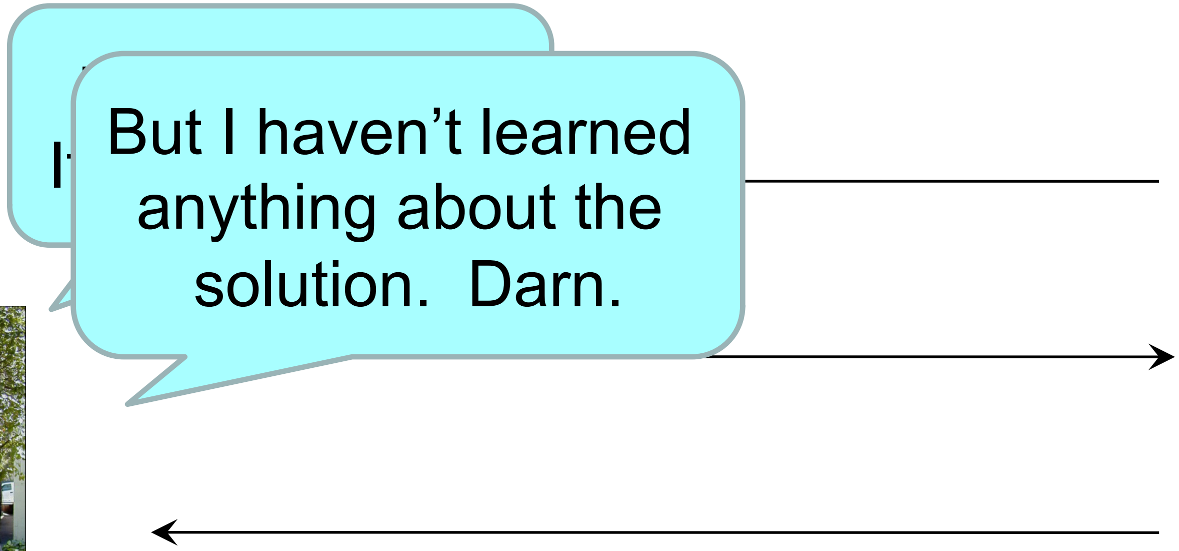


8	3	5	4	1	6	9	2	7
2	9	6	8	5	7	4	3	1
4	1	7	2	9	3	6	5	8
5	6	9	1	3	4	7	8	2
1	2	3	6	7	8	5	4	9
7	4	8	5	2	9	1	6	3
6	5	2	7	8	1	3	9	4
9	8	1	3	4	5	2	7	6
3	7	4	9	6	2	8	1	5

Goal: Prove the puzzle is solvable

8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

8	3	5	4	1	6	9	2	7
2	9	6	8	5	7	4	3	1
4	1	7	2	9	3	6	5	8
5	6	9	1	3	4	7	8	2
1	2	3	6	7	8	5	4	9
7	4	8	5	2	9	1	6	3
6	5	2	7	8	1	3	9	4
9	8	1	3	4	5	2	7	6
3	7	4	9	6	2	8	1	5



But I haven't learned anything about the solution. Darn.

Verifier

Prover

David Wagner, UC Berkeley

You prepare your proof

8	3	5	**4**	1	**6**	9	2	**7**
2	9	6	8	5	7	**4**	3	1
4	**1**	7	2	9	3	**6**	**5**	8
5	6	**9**	1	**3**	4	**7**	**8**	2
1	2	3	6	**7**	8	5	4	9
7	**4**	**8**	5	**2**	9	**1**	6	**3**
6	**5**	**2**	7	8	1	3	**9**	4
9	8	**1**	3	4	5	2	7	6
3	7	4	**9**	6	**2**	8	1	**5**

1 →	e
2 →	h
3 →	c
4 →	f
5 →	i
6 →	d
7 →	b
8 →	a
9 →	g

8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

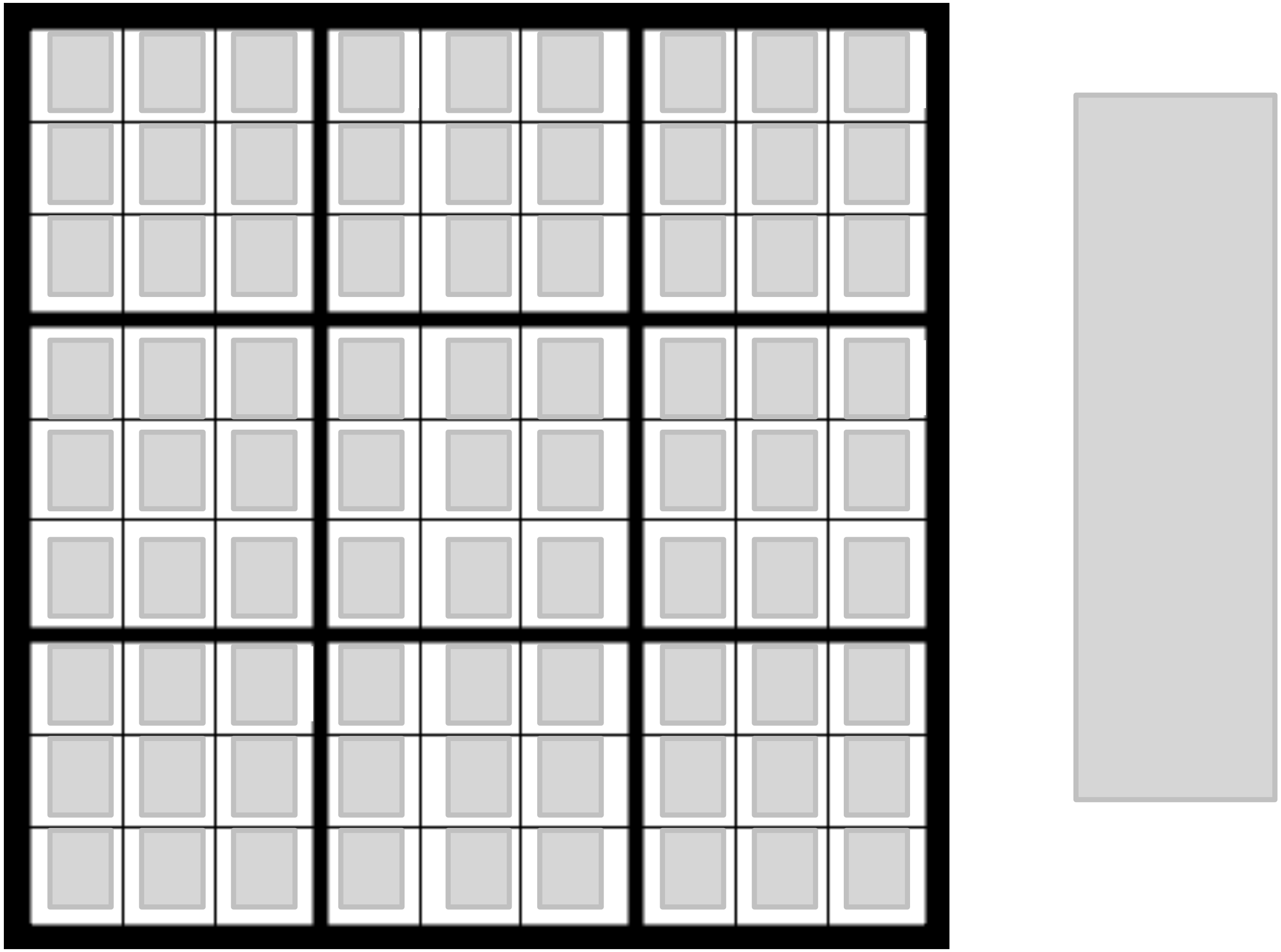
You prepare your proof

a	c	i	f	e	d	g	h	b
h	g	d	a	i	b	f	c	e
f	e	b	h	g	c	d	i	a
i	d	g	e	c	f	b	a	h
e	h	c	d	b	a	i	f	g
b	f	a	i	h	g	e	d	c
d	i	h	b	a	e	c	g	f
g	a	e	c	f	i	h	b	d
c	b	f	g	d	h	a	e	i

1	→	e
2	→	h
3	→	c
4	→	f
5	→	i
6	→	d
7	→	b
8	→	a
9	→	g

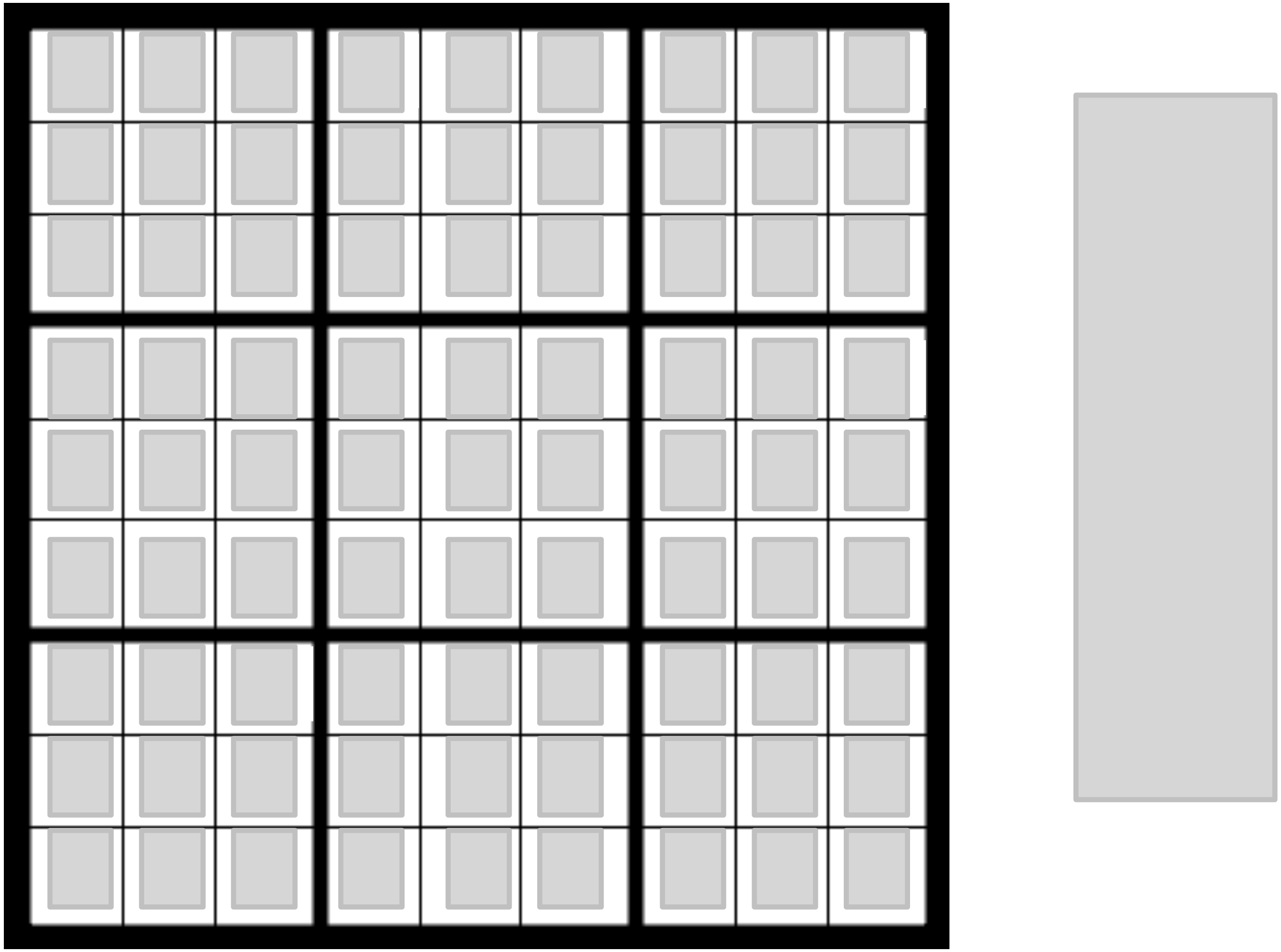
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

You prepare your proof



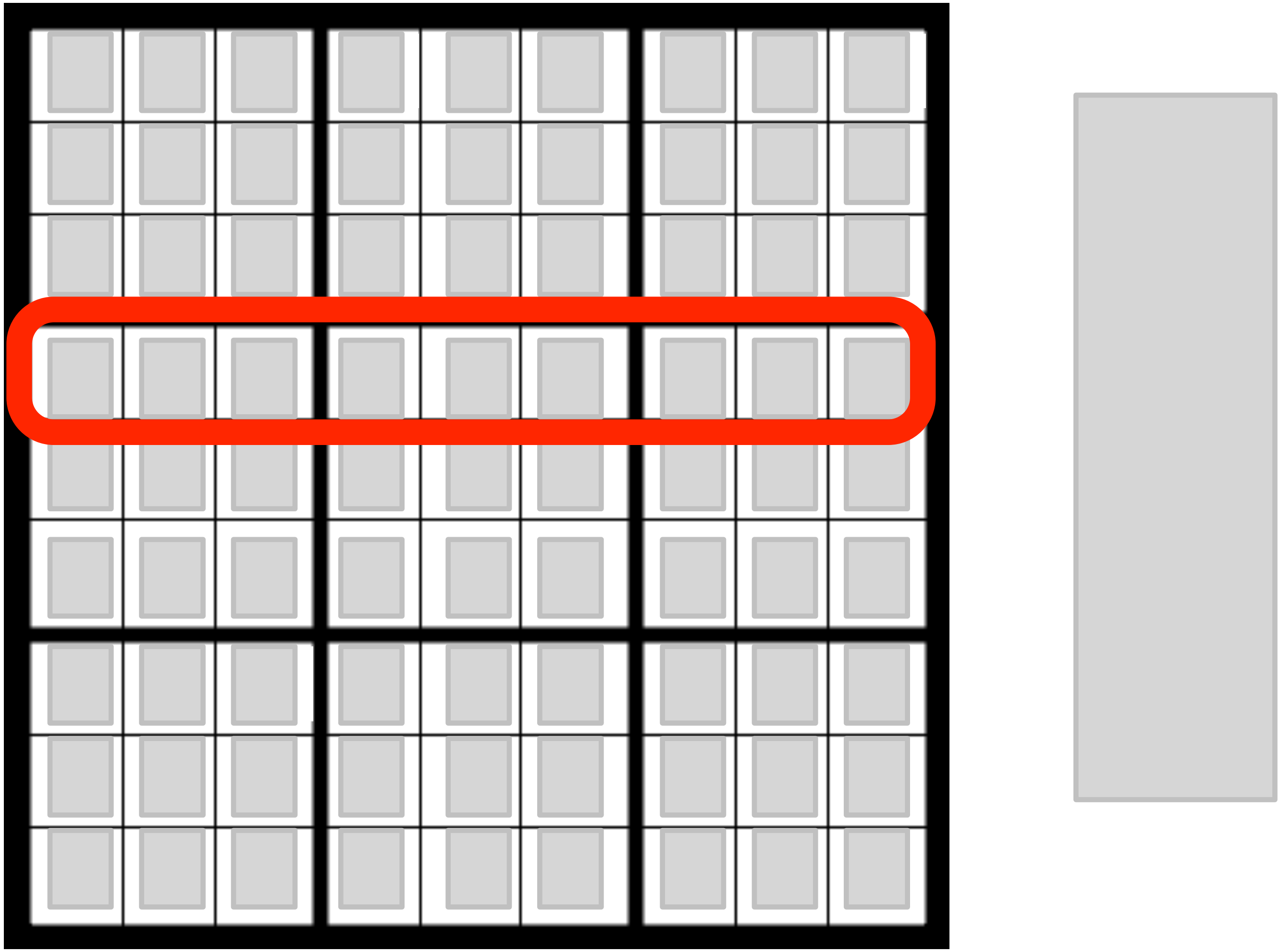
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest



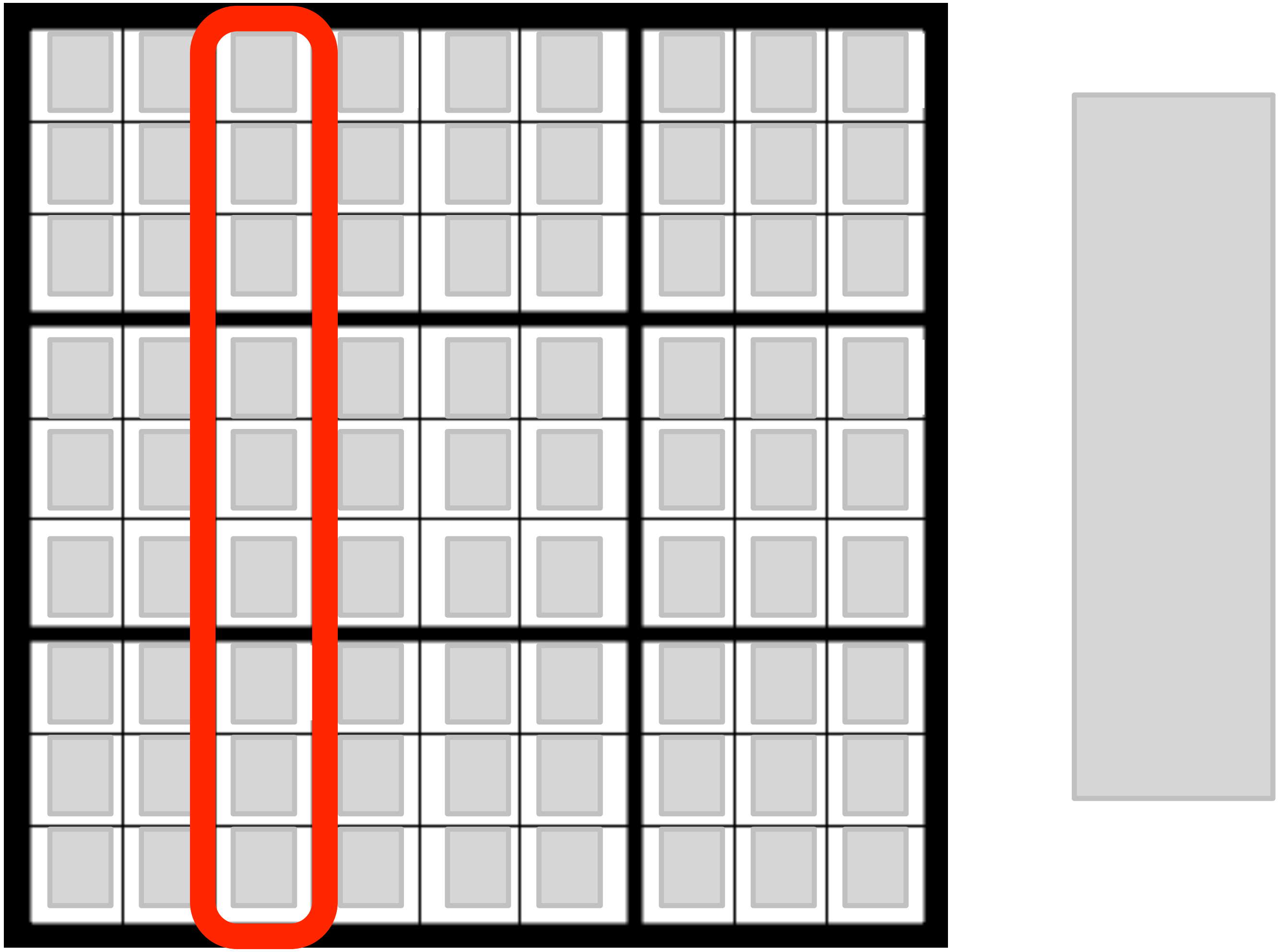
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest (option 1)



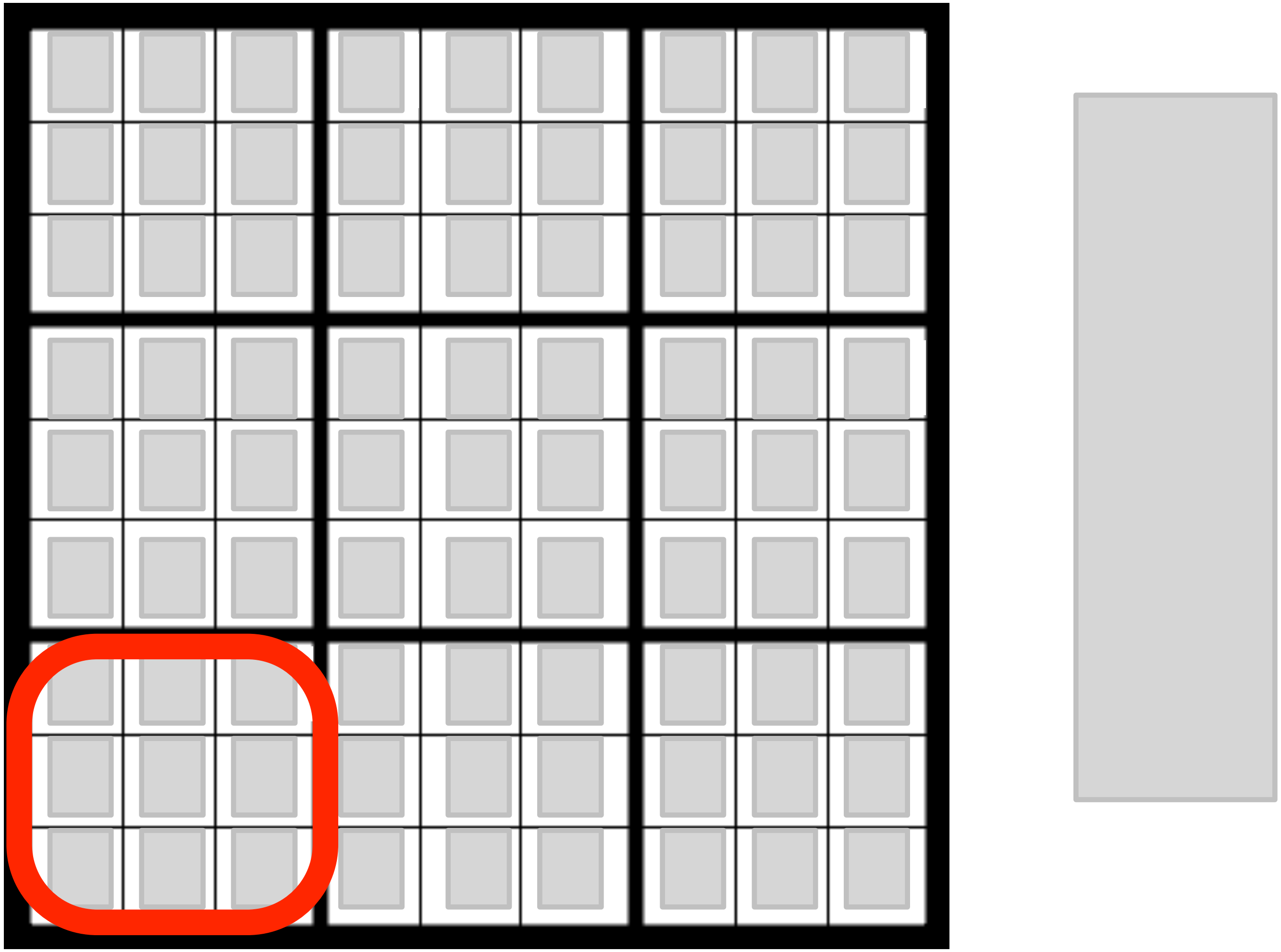
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest (option 2)



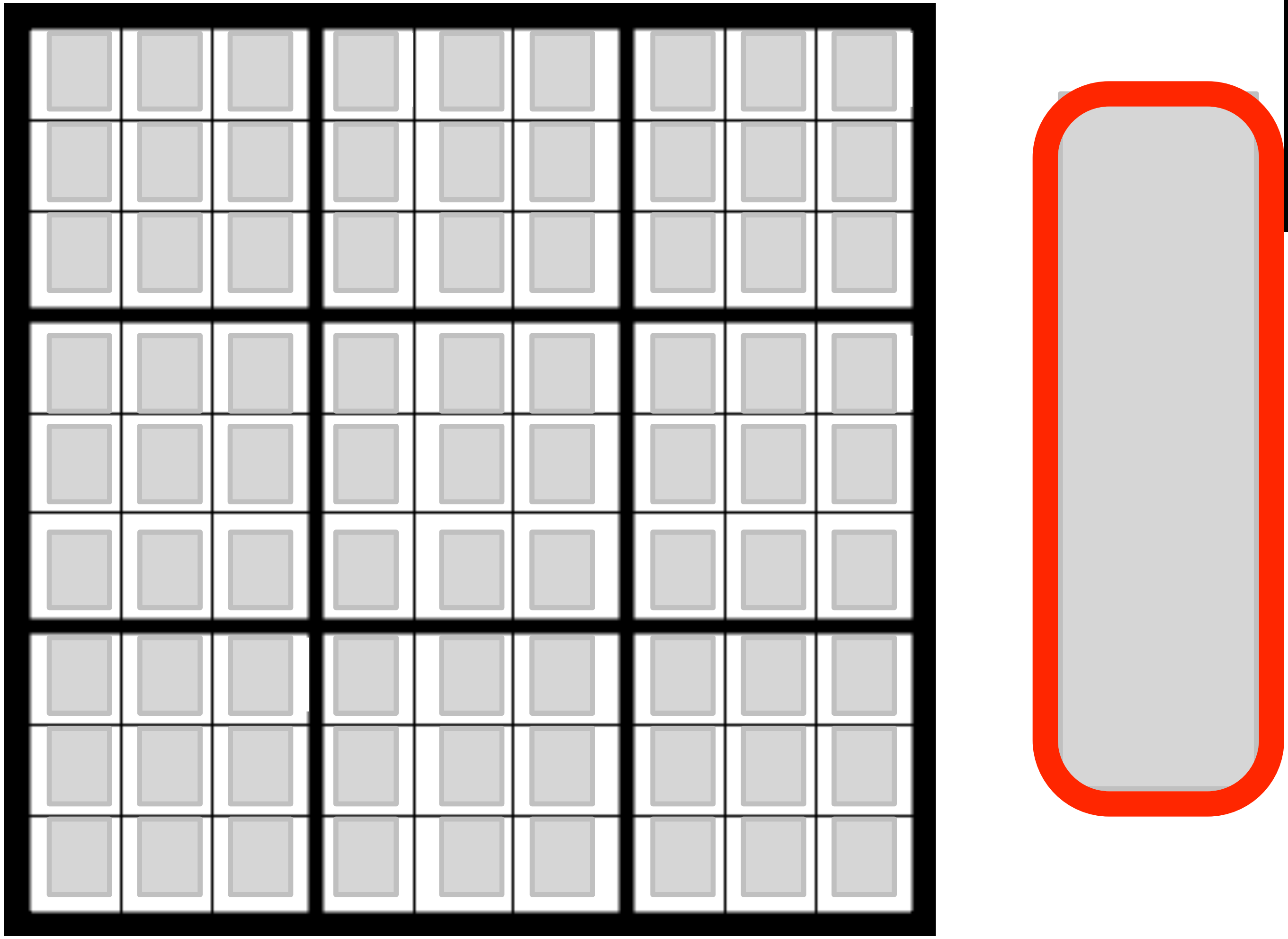
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest (option 3)



8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest (option 4)

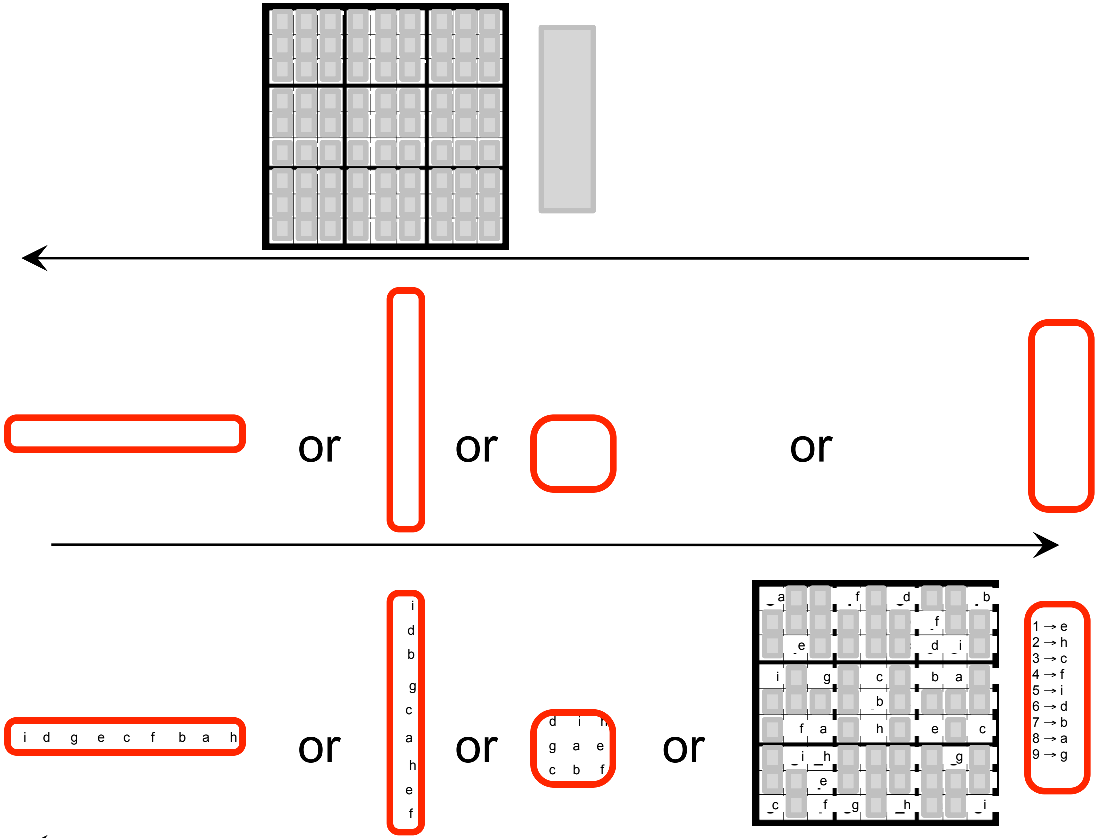


8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

Zero-knowledge proof: puzzle is solvable

8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

8	3	5	4	1	6	9	2	7
2	9	6	8	5	7	4	3	1
4	1	7	2	9	3	6	5	8
5	6	9	1	3	4	7	8	2
1	2	3	6	7	8	5	4	9
7	4	8	5	2	9	1	6	3
6	5	2	7	8	1	3	9	4
9	8	1	3	4	5	2	7	6
3	7	4	9	6	2	8	1	5



Verifier

Prover

Repeat 1000 times

David Wagner, UC Berkeley

Goal: Prove the puzzle is solvable

8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

I’m convinced!
It can be solved!

But I haven’t learned anything about the solution. Darn.

Verifier

8	3	5	4	1	6	9	2	7
2	9	6	8	5	7	4	3	1
4	1	7	2	9	3	6	5	8
5	6	9	1	3	4	7	8	2
1	2	3	6	7	8	5	4	9
7	4	8	5	2	9	1	6	3
6	5	2	7	8	1	3	9	4
9	8	1	3	4	5	2	7	6
3	7	4	9	6	2	8	1	5

Prover

Summary

Alice can prove to Dave that the Sudoku puzzle has a solution.
Dave gains zero knowledge about the solution.

Sudoku isn’t special:

Theorem. If I can prove it, I can prove it to you without revealing the proof.

Summary

Theorem. If I can prove it, I can prove it to you without revealing the proof.

Electronic voting

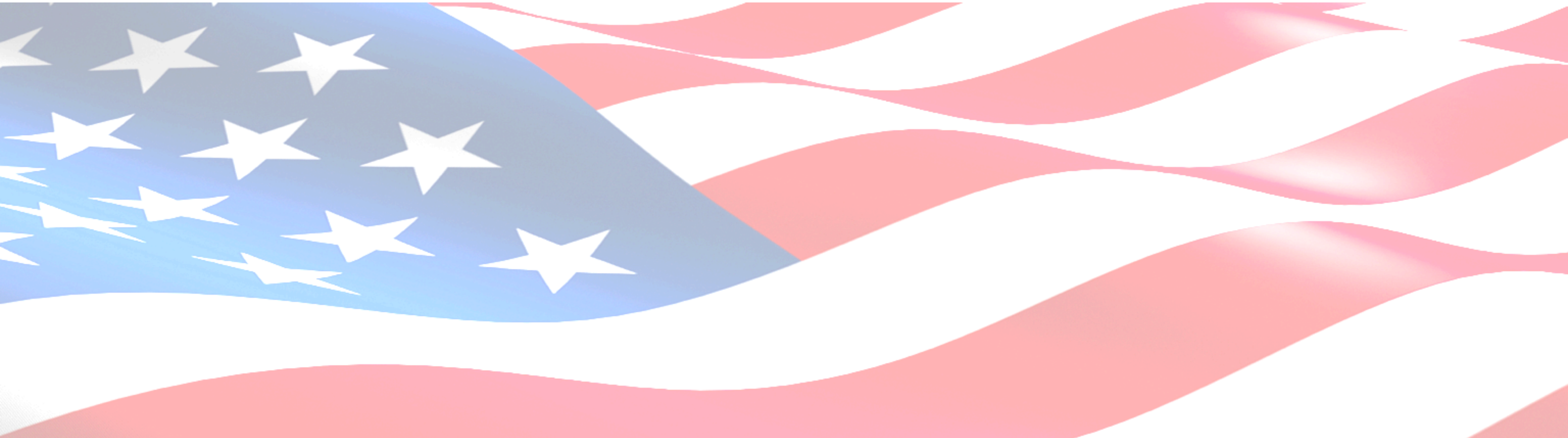
For 25% of overseas and military voters, their vote doesn’t count, because the mail is too slow and unreliable.

OVERSEAS VOTE FOUNDATION

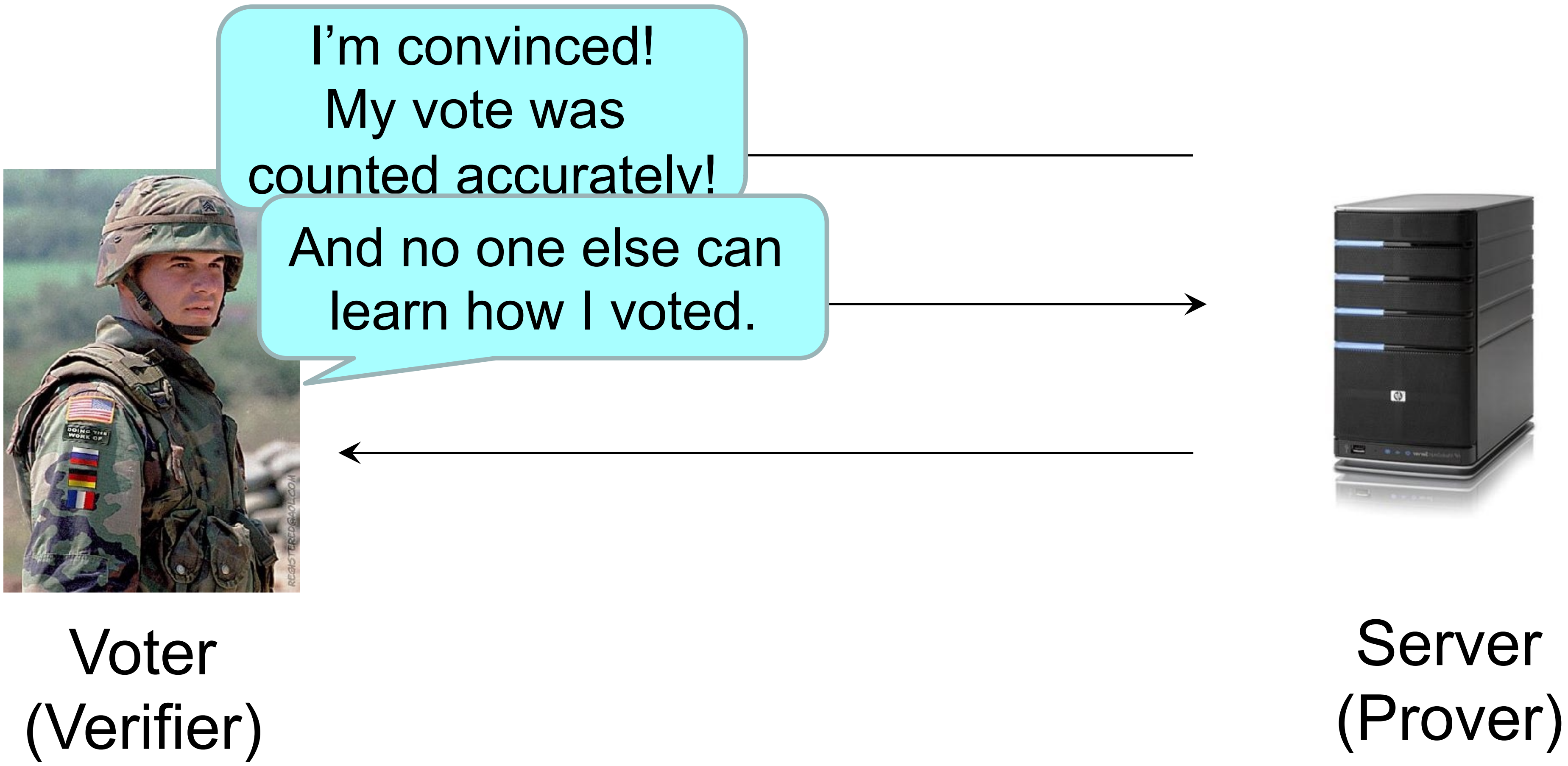
Electronic voting

What about voting over the Internet?

It solves the problem with the mail, but introduces new problems: how do we trust or verify the result?



Research: Trustworthy Remote Voting



I'm convinced!
My vote was
counted accurately!

And no one else can
learn how I voted.

Voter
(Verifier)

Server
(Prover)