



# Casting votes in the Auditorium

**Daniel Sandler and Dan S. Wallach**  
Rice University

2007 USENIX/ACCURATE Electronic Voting Technology Workshop

e-voting research

**GREATEST HITS**

- 1 Current DREs have problems and should not be trusted**
- 2 We can build voting systems that are more trustworthy**

# **1 Current DREs have problems and should not be trusted**

*Kohno et al. 2004, Hursti 2006, Wagner et al. 2006, Feldman et al. 2007, Gonggrijp et al. 2007, ...*

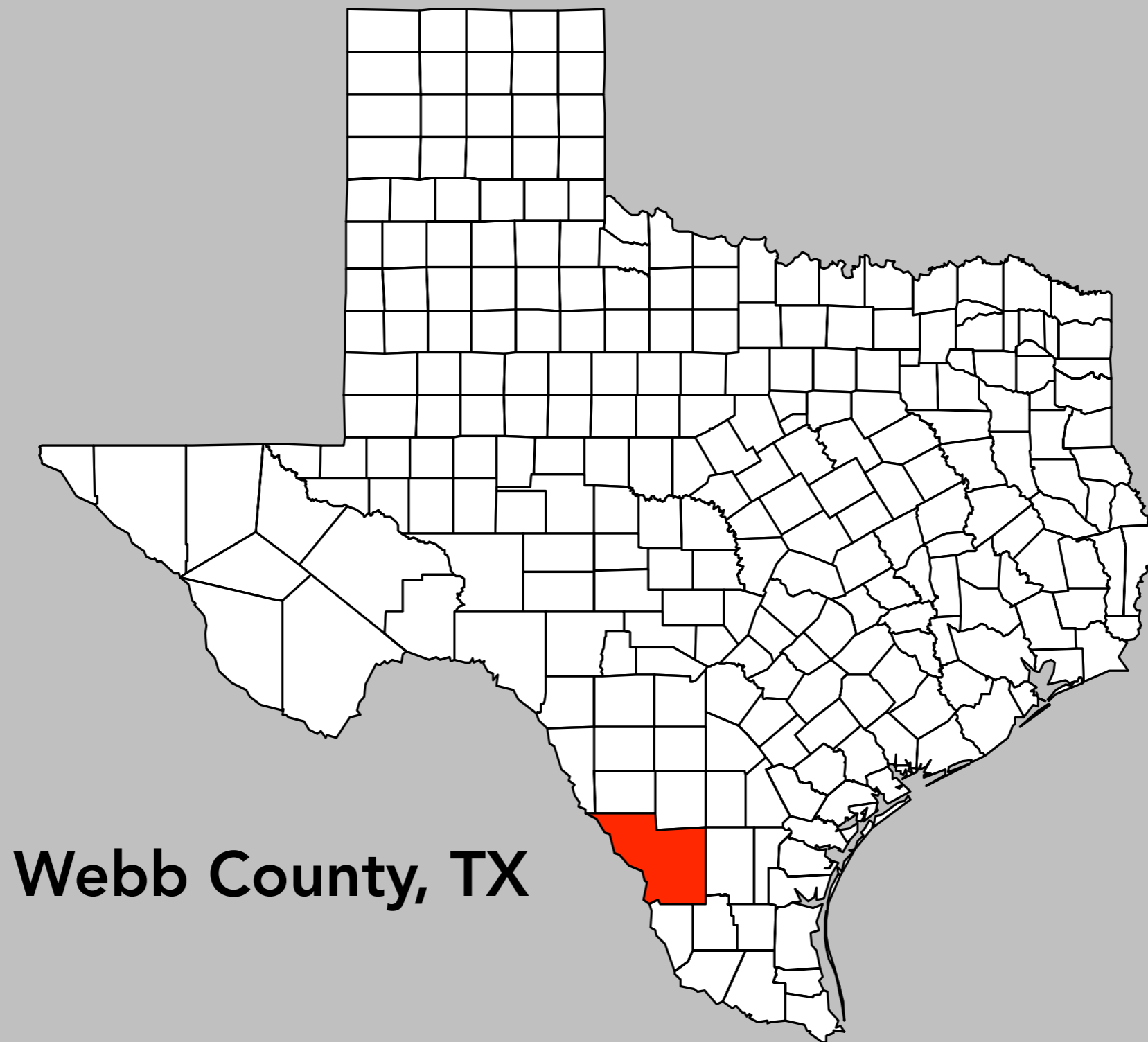
# **2 We can build voting systems that are more trustworthy**

*Benaloh 2006, Molnar et al. 2006, Yee 2006, Sastry 2006, ...*

Let's talk about  
something else.

# What I Did Over Spring Break (March 2006)

by Dan S. + Dan W.

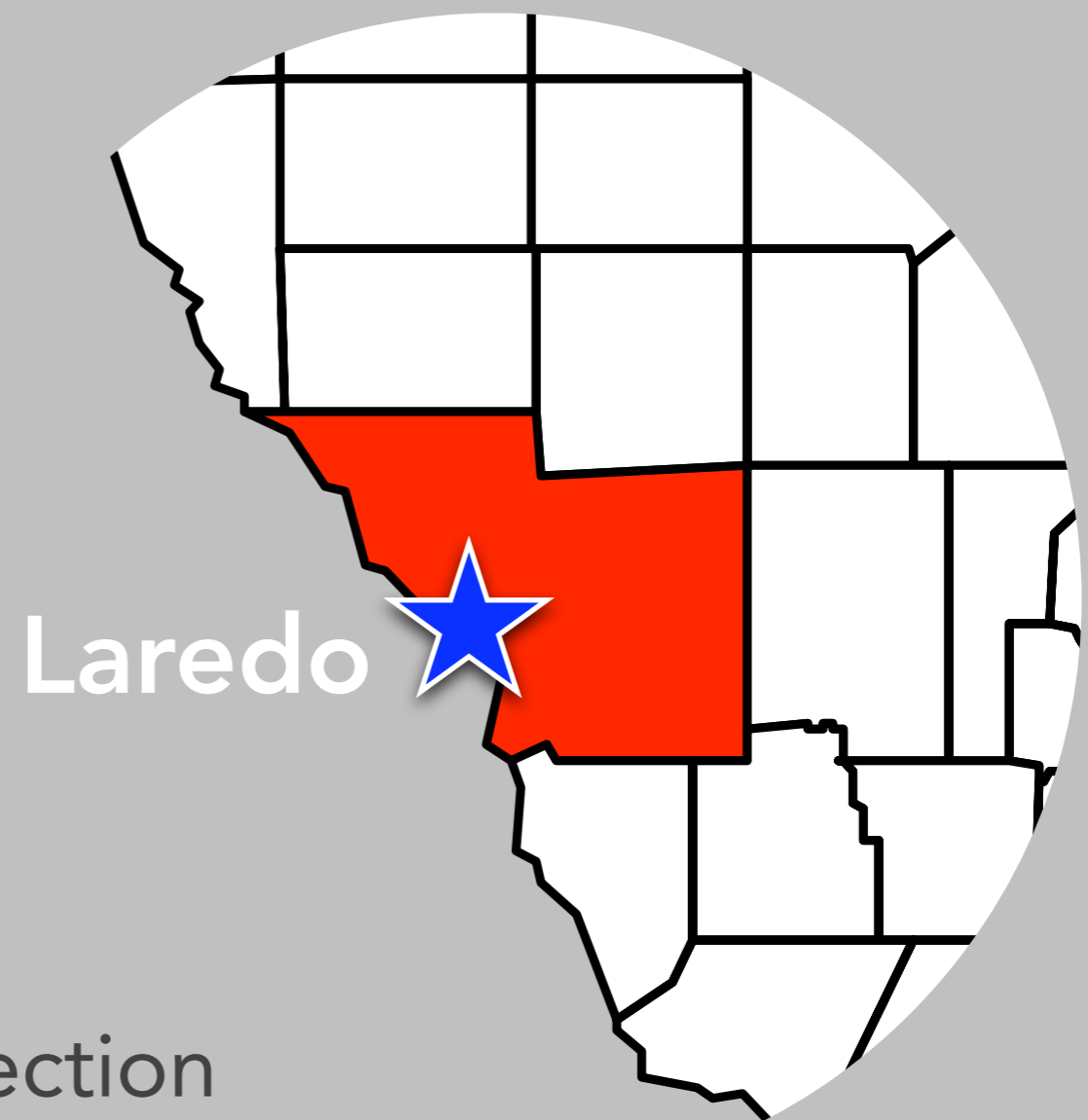


**Webb County, TX**

**March 7, 2006:**

2006 Democratic primary election

(County's first use of DREs)



# An unusual situation

**Voters given a choice:**

# An unusual situation

Voters given a choice:



DRE

(ES&S iVotronic)

# An unusual situation

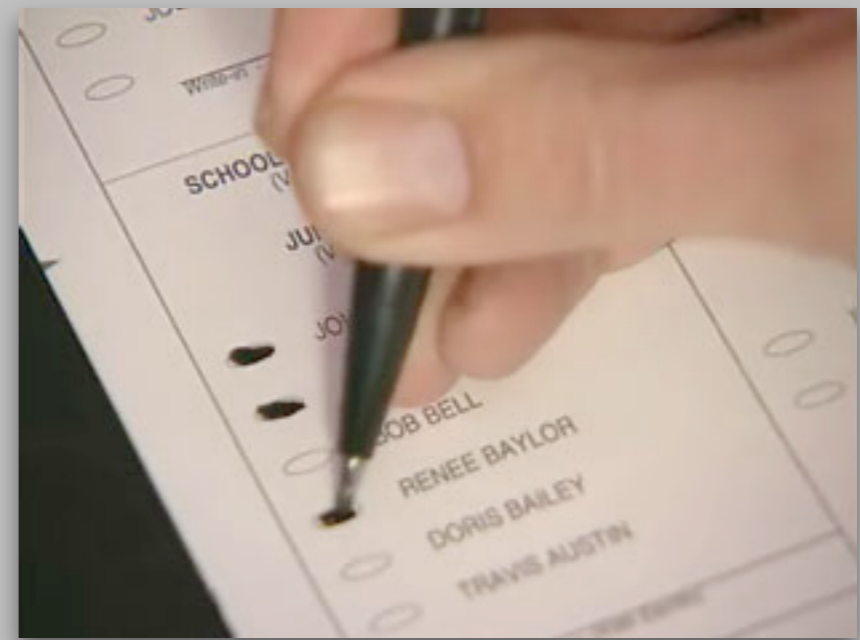
Voters given a choice:



DRE

(ES&S iVotronic)

OR



Paper

(central ES&S op-scan)

# Flores v. Lopez

# Flores v. Lopez

**~50,000 votes cast**

# Flores v. Lopez

**~50,000 votes cast**

**Margin of victory: ~100 votes**

# Flores v. Lopez

**~50,000 votes cast**

**Margin of victory: ~100 votes**

**The loser suspected the DREs**

...because he looked better on paper

# Flores v. Lopez

**~50,000 votes cast**

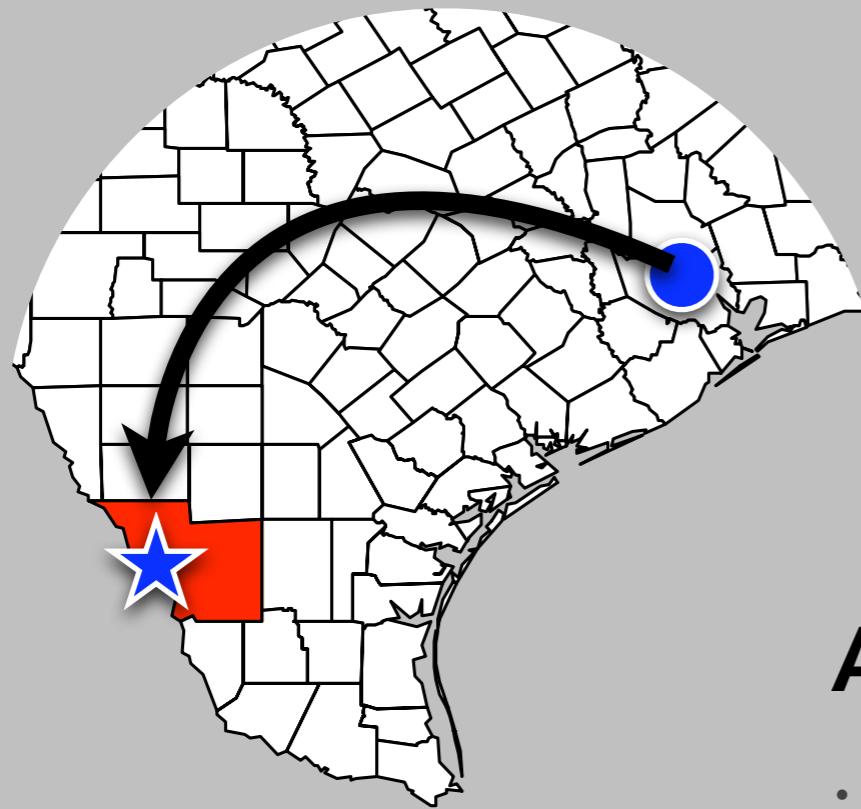
**Margin of victory: ~100 votes**

**The loser suspected the DREs**

...because he looked better on paper

**Lawsuit**

**Bring in the experts!**



**April 12–13**

initial investigation (Dan & Dan)

# Webb Co. data

# Webb Co. data

**Raw binary data from Compact Flash cards**

Opaque, undocumented format

# Webb Co. data

**Raw binary data from Compact Flash cards**

Opaque, undocumented format

**Text output from DRE tabulator**

For each machine:

“IMAGELOG.TXT” (cast ballots)

“EVENTLOG.TXT” (more on that later)



A smoking gun?

A smoking gun?  
Evidence of evil DREs?

A smoking gun?  
Evidence of evil DREs?  
**HACKS???**

A smoking gun?  
Evidence of evil DREs?  
**HACKS???**

(how could we?)

# What we (really) found

## Anomalies in the **event logs**

Per-machine records

List of important election events

e.g. "terminal open," "ballot cast," ...

# Example event log

Votronic	PEB#	Type	Date	Time	Event
5140052	161061	SUP	03/07/2006	15:29:03	01 Terminal clear and test
	160980	SUP	03/07/2006	15:31:15	09 Terminal open
			03/07/2006	15:34:47	13 Print zero tape
			03/07/2006	15:36:36	13 Print zero tape
	160999	SUP	03/07/2006	15:56:50	20 Normal ballot cast
			03/07/2006	16:47:12	20 Normal ballot cast
			03/07/2006	18:07:29	20 Normal ballot cast
			03/07/2006	18:17:03	20 Normal ballot cast
			03/07/2006	18:37:24	22 Super ballot cancel
			03/07/2006	18:41:18	20 Normal ballot cast
			03/07/2006	18:46:23	20 Normal ballot cast
	160980	SUP	03/07/2006	19:07:14	10 Terminal close

# Example event log

Votronic	PEB#	Type	Date	Time	Event
5140052	161061	SUP	03/07/2006	15:29:03	01 Terminal clear and test
	160980	SUP	03/07/2006	15:31:15	09 Terminal open
			03/07/2006	15:34:47	13 Print zero tape
			03/07/2006	15:36:36	13 Print zero tape
	160999	SUP	03/07/2006	15:56:50	20 Normal ballot cast
			03/07/2006	16:47:12	20 Normal ballot cast
			03/07/2006	18:07:29	20 Normal ballot cast
			03/07/2006	18:17:03	20 Normal ballot cast
			03/07/2006	18:37:24	22 Super ballot cancel
			03/07/2006	18:41:18	20 Normal ballot cast
			03/07/2006	18:46:23	20 Normal ballot cast
	160980	SUP	03/07/2006	19:07:14	10 Terminal close

# Example event log

Votronic	PEB#	Type	Date	Time	Event
5140052	161061	SUP	03/07/2006	15:29:03	01 Terminal clear and test
	160980	SUP	03/07/2006	15:31:15	09 Terminal open
			03/07/2006	15:34:47	13 Print zero tape
			03/07/2006	15:36:36	13 Print zero tape
	160999	SUP	03/07/2006	15:56:50	20 Normal ballot cast
			03/07/2006	16:47:12	20 Normal ballot cast
			03/07/2006	18:07:29	20 Normal ballot cast
			03/07/2006	18:17:03	20 Normal ballot cast
			03/07/2006	18:37:24	22 Super ballot cancel
			03/07/2006	18:41:18	20 Normal ballot cast
			03/07/2006	18:46:23	20 Normal ballot cast
	160980	SUP	03/07/2006	19:07:14	10 Terminal close

# Example event log

Votronic	PEB#	Type	Date	Time	Event
5140052	161061	SUP	03/07/2006	15:29:03	01 Terminal clear and test
	160980	SUP	03/07/2006	15:31:15	09 Terminal open
			03/07/2006	15:34:47	13 Print zero tape
			03/07/2006	15:36:36	13 Print zero tape
	160999	SUP	03/07/2006	15:56:50	20 Normal ballot cast
			03/07/2006	16:47:12	20 Normal ballot cast
			03/07/2006	18:07:29	20 Normal ballot cast
			03/07/2006	18:17:03	20 Normal ballot cast
			03/07/2006	18:37:24	22 Super ballot cancel
			03/07/2006	18:41:18	20 Normal ballot cast
			03/07/2006	18:46:23	20 Normal ballot cast
	160980	SUP	03/07/2006	19:07:14	10 Terminal close

# Example event log

Votronic	PEB#	Type	Date	Time	Event
5140052	161061	SUP	03/07/2006	15:29:03	01 Terminal clear and test
	160980	SUP	03/07/2006	15:31:15	09 Terminal open
			03/07/2006	15:34:47	13 Print zero tape
			03/07/2006	15:36:36	13 Print zero tape
	160999	SUP	03/07/2006	15:56:50	20 Normal ballot cast
			03/07/2006	16:47:12	20 Normal ballot cast
			03/07/2006	18:07:29	20 Normal ballot cast
			03/07/2006	18:17:03	20 Normal ballot cast
			03/07/2006	18:37:24	22 Super ballot cancel
			03/07/2006	18:41:18	20 Normal ballot cast
			03/07/2006	18:46:23	20 Normal ballot cast
	160980	SUP	03/07/2006	19:07:14	10 Terminal close

# Example event log

Votronic	PEB#	Type	Date	Time	Event
5140052	161061	SUP	03/07/2006	15:29:03	01 Terminal clear and test
	160980	SUP	03/07/2006	15:31:15	09 Terminal open
			03/07/2006	15:34:47	13 Print zero tape
			03/07/2006	15:36:36	13 Print zero tape
	160999	SUP	03/07/2006	15:56:50	20 Normal ballot cast
			03/07/2006	16:47:12	20 Normal ballot cast
			03/07/2006	18:07:29	20 Normal ballot cast
			03/07/2006	18:17:03	20 Normal ballot cast
			03/07/2006	18:37:24	22 Super ballot cancel
			03/07/2006	18:41:18	20 Normal ballot cast
			03/07/2006	18:46:23	20 Normal ballot cast
	160980	SUP	03/07/2006	19:07:14	10 Terminal close

# Problem #1

## Logs starting mid-day

```
03/07/2006 15:29:03 Terminal clear and test  
03/07/2006 15:31:15 Terminal open
```

# Problem #1

## Logs starting mid-day

```
03/07/2006 15:29:03 Terminal clear and test
03/07/2006 15:31:15 Terminal open
```

Polls opened around **7 AM** across Webb Co.

What happened between 7 and 3:30?

**Lost votes?**

# Problem #1

## Logs starting mid-day

```
03/07/2006 15:29:03 Terminal clear and test  
03/07/2006 15:31:15 Terminal open
```

Polls opened around **7 AM** across Webb Co.

What happened between 7 and 3:30?

**Lost votes?**

(10 total machines)

# Problem #2

## Election events on wrong day

Votronic	PEB#	Type	Date	Time	Event
5142523	161061	SUP	02/26/2006	19:07:05	01 Terminal clear and test
	161115	SUP	03/06/2006	06:57:23	09 Terminal open
			03/06/2006	07:01:47	13 Print zero tape
			03/06/2006	07:03:41	13 Print zero tape
	161109	SUP	03/06/2006	10:08:26	20 Normal ballot cast
					[... 9 more ballots cast ...]
	161115	SUP	03/06/2006	19:29:00	27 Override
			03/06/2006	19:29:00	10 Terminal close

# Problem #2

## Election events on wrong day

Votronic	PEB#	Type	Date	Time	Event
5142523	161061	SUP	02/26/2006	19:07:05	01 Terminal clear and test
	161115	SUP	03/06/2006	06:57:23	09 Terminal open
			03/06/2006	07:01:47	13 Print zero tape
			03/06/2006	07:03:41	13 Print zero tape
	161109	SUP	03/06/2006	10:08:26	20 Normal ballot cast
					[... 9 more ballots cast ...]
	161115	SUP	03/06/2006	19:29:00	27 Override
			03/06/2006	19:29:00	10 Terminal close

# Problem #2

## Election events on wrong day

Votronic	PEB#	Type	Date	Time	Event
5142523	161061	SUP	02/26/2006	19:07:05	01 Terminal clear and test
	161115	SUP	03/06/2006	06:57:23	09 Terminal open
			03/06/2006	07:01:47	13 Print zero tape
			03/06/2006	07:03:41	13 Print zero tape
	161109	SUP	03/06/2006	10:08:26	20 Normal ballot cast
					[... 9 more ballots cast ...]
	161115	SUP	03/06/2006	19:29:00	27 Override
			03/06/2006	19:29:00	10 Terminal close

The election was held on 03/07!

# Problem #2

## Election events on wrong day

Votronic	PEB#	Type	Date	Time	Event
5142523	161061	SUP	02/26/2006	19:07:05	01 Terminal clear and test
	161115	SUP	03/06/2006	06:57:23	09 Terminal open
			03/06/2006	07:01:47	13 Print zero tape
			03/06/2006	07:03:41	13 Print zero tape
	161109	SUP	03/06/2006	10:08:26	20 Normal ballot cast
					[... 9 more ballots cast ...]
	161115	SUP	03/06/2006	19:29:00	27 Override
			03/06/2006	19:29:00	10 Terminal close

The election was held on 03/07!  
(4 machines / 41 votes)

Votronic	PEB#	Type	Date	Time	Event
5145172	161061	SUP	03/06/2006	15:04:09	01 Terminal clear and test
	161126	SUP	03/06/2006	15:19:34	09 Terminal open
	160973	SUP	03/06/2006	15:26:59	20 Normal ballot cast
			03/06/2006	15:30:39	20 Normal ballot cast
	161126	SUP	03/06/2006	15:38:37	27 Override
			03/06/2006	15:38:37	10 Terminal close

Votronic	PEB#	Type	Date	Time	Event
5145172	161061	SUP	03/06/2006	15:04:09	01 Terminal clear and test
	161126	SUP	03/06/2006	15:19:34	09 Terminal open
	160973	SUP	03/06/2006	15:26:59	20 Normal ballot cast
			03/06/2006	15:30:39	20 Normal ballot cast
	161126	SUP	03/06/2006	15:38:37	27 Override
			03/06/2006	15:38:37	10 Terminal close

Votronic	PEB#	Type	Date	Time	Event
5145172	161061	SUP	03/06/2006	15:04:09	01 Terminal clear and test
	161126	SUP	03/06/2006	15:19:34	09 Terminal open
	160973	SUP	03/06/2006	15:26:59	20 Normal ballot cast
			03/06/2006	15:30:39	20 Normal ballot cast
	161126	SUP	03/06/2006	15:38:37	27 Override
			03/06/2006	15:38:37	10 Terminal close

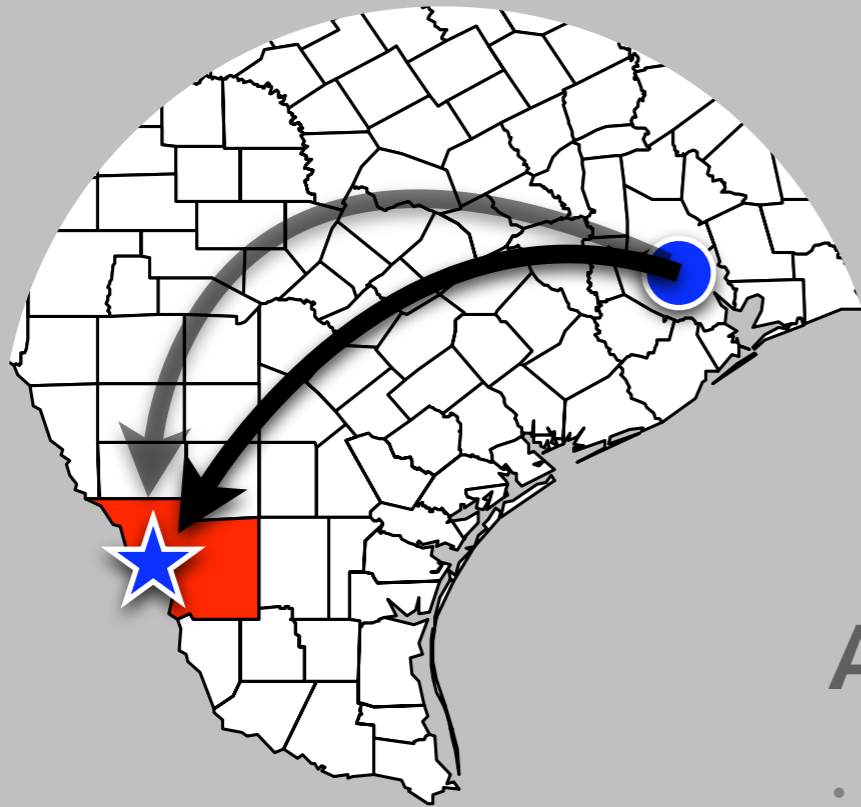
26 machines with exactly two  
ballots cast the day before

Votronic	PEB#	Type	Date	Time	Event
5145172	161061	SUP	03/06/2006	15:04:09	01 Terminal clear and test
	161126	SUP	03/06/2006	15:19:34	09 Terminal open
	160973	SUP	03/06/2006	15:26:59	20 Normal ballot cast
			03/06/2006	15:30:39	20 Normal ballot cast
	161126	SUP	03/06/2006	15:38:37	27 Override
			03/06/2006	15:38:37	10 Terminal close

26 machines with exactly two ballots cast the day before

We learned that these were probably L&A test votes, erroneously included in the tally

(52 votes)



**April 12–13**

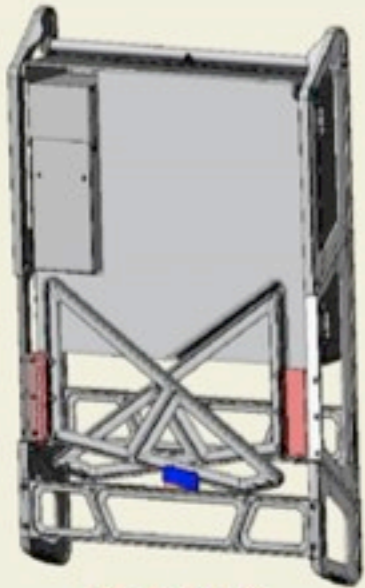
initial investigation (Dan & Dan)

**April 24–25**

follow-up trip (just Dan)



## BOOTH SETUP SEQUENCE



Delivered



Fold out legs



Pivot up platform  
and lock upright



Unlock privacy  
screens and add iVotronic

# History for Laredo, TX

Tuesday, April 25, 2006 — [View Current Conditions](#)

## Daily Summary

[« Previous Day](#)

April

25

2006

Go

[Next Day »](#)

**Daily**

[Weekly](#)

[Monthly](#)

[Custom](#)

**Actual:**

**Average :**

**Record :**

### Temperature:

Mean Temperature

87 °F / 30 °C

-

Max Temperature

101 °F / 38 °C

85 °F / 29 °C

101 °F / 38 °C (2006)

Min Temperature

73 °F / 22 °C

64 °F / 17 °C

55 °F / 12 °C (2001)

source: [wunderground.com](http://wunderground.com)



**Machines containing only two votes**

Everything appeared normal

Most likely L&A test votes

## **Machines containing only two votes**

Everything appeared normal

Most likely L&A test votes

## **Others**

Hardware clock set incorrectly

Just enough to account for anomaly

## **Machines containing only two votes**

Everything appeared normal

Most likely L&A test votes

## **Others**

Hardware clock set incorrectly

Just enough to account for anomaly

**This is not proof of correct behavior!**

# Problem #3

## Insufficient audit data

**We couldn't collect data from every machine**

Many were cleared after the election!

(Only the CF card "dumps" remain.)

**Paper records missing**

Zero tapes

Cancelled ballot logs

# Observations

**“Mistakes were made.”**



## **Violations of election procedures**

Counting test votes in final results

Loss of zero tapes and other paper logs

Erasure of some machines

## **Violations of election procedures**

Counting test votes in final results

Loss of zero tapes and other paper logs

Erasure of some machines

## **Local (mis)configuration**

Hardware clocks set wrong

## **Violations of election procedures**

Counting test votes in final results

Loss of zero tapes and other paper logs

Erasement of some machines

## **Local (mis)configuration**

Hardware clocks set wrong

**These things cast doubt on the results**



Honest mistakes  
or illegitimate votes?

Honest mistakes  
or illegitimate votes?

**No way to be sure.**

Honest mistakes  
or illegitimate votes?

No way to be sure.

**Believable audits impossible.**

**These things happen  
in real elections.**

# Research goals

# Research goals

Make it **easier to audit results** after election day

# Research goals

Make it **easier to audit results** after election day

Make it **harder to make mistakes** on election day



**Prove**

every vote tallied is valid

every valid vote is present

## Prove

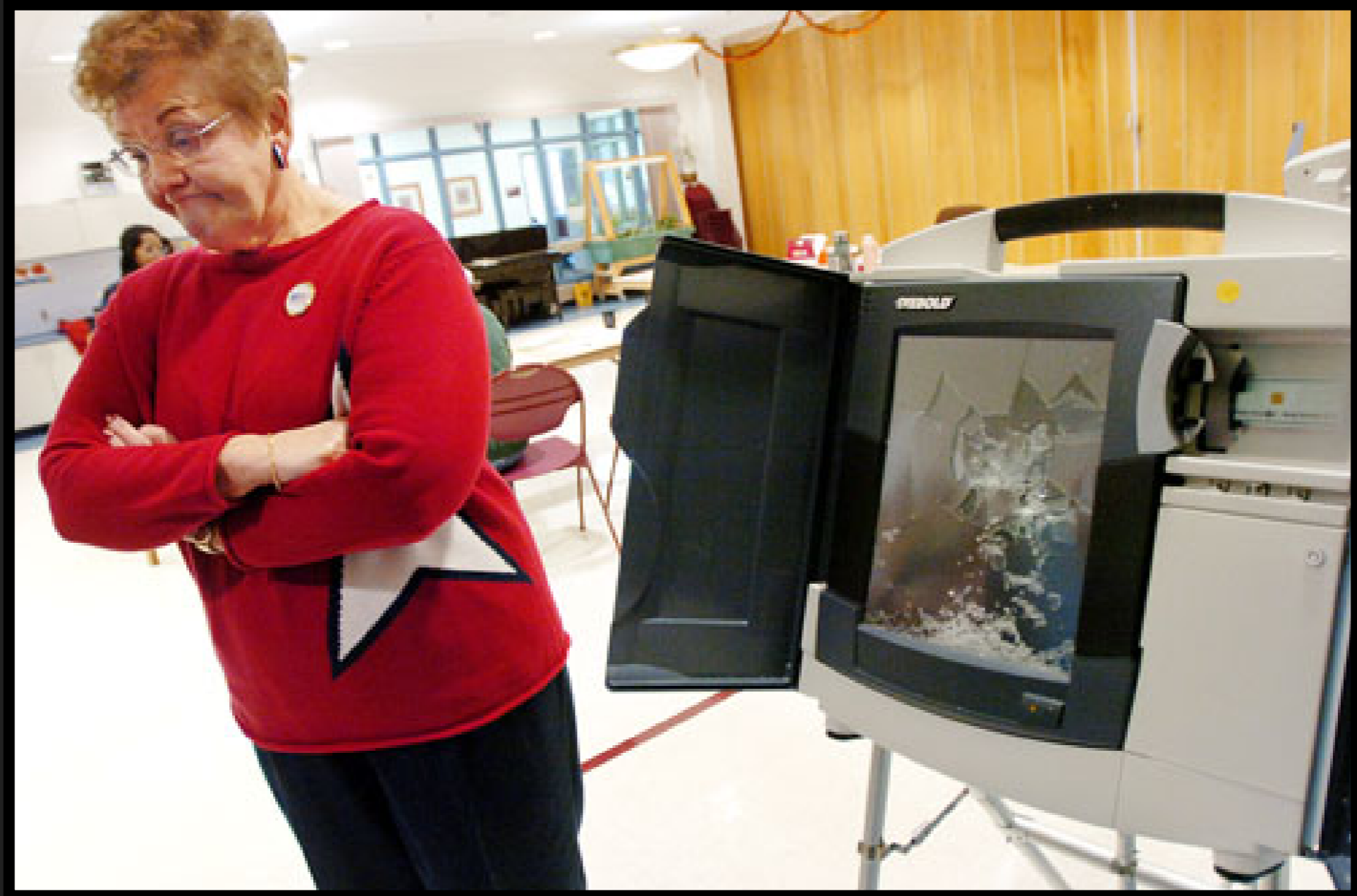
every vote tallied is valid

every valid vote is present

## Tolerate

accidental loss/deletion of records

election-day machine failure



**How?**

**Connect the machines  
together.**

# Benefits of the network

## **Store everything everywhere**

Massive redundancy

Stop trusting DREs to keep their own audit data

## **Link all votes, events together**


Create a secure timeline of election events

Tamper-evident proof of each vote's legitimacy

# Auditorium

# Ingredient: hash chains

```
“Machine turned on” (HASH = 0x1234)
“Cast a vote after event 0x1234” (HASH = 0xABCD)
“Cast a vote after event 0xABCD” (HASH = 0xBEEF)
“Turned off after event 0xBEEF” (HASH = 0x4242)
```



**Every event includes the hash of a previous event**  
 (“hash chaining”)

Result: **precedence** — “X must have happened after Y”

**To alter or delete a single record,**

you must alter every subsequent event as well

# Ingredient #2: timeline entanglement

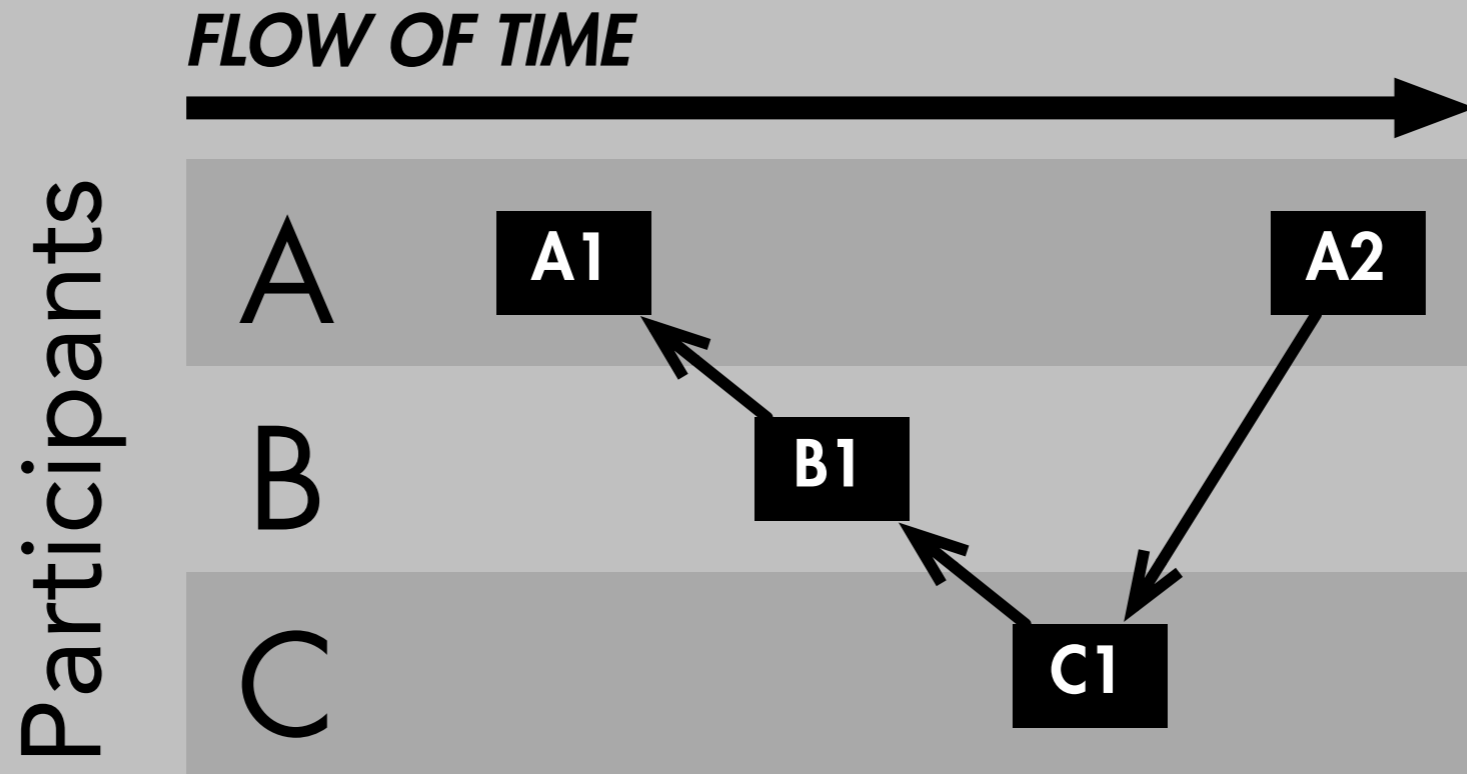
**Entanglement = "chain with hashes from others"**

Result: event precedence between participants

**Malicious machines can't retroactively alter their logs**

This would upset the global timeline!





B1 incorporates  $\text{HASH}(A1)$   
C1 incorporates  $\text{HASH}(B1)$   
A2 incorporates  $\text{HASH}(C1)$

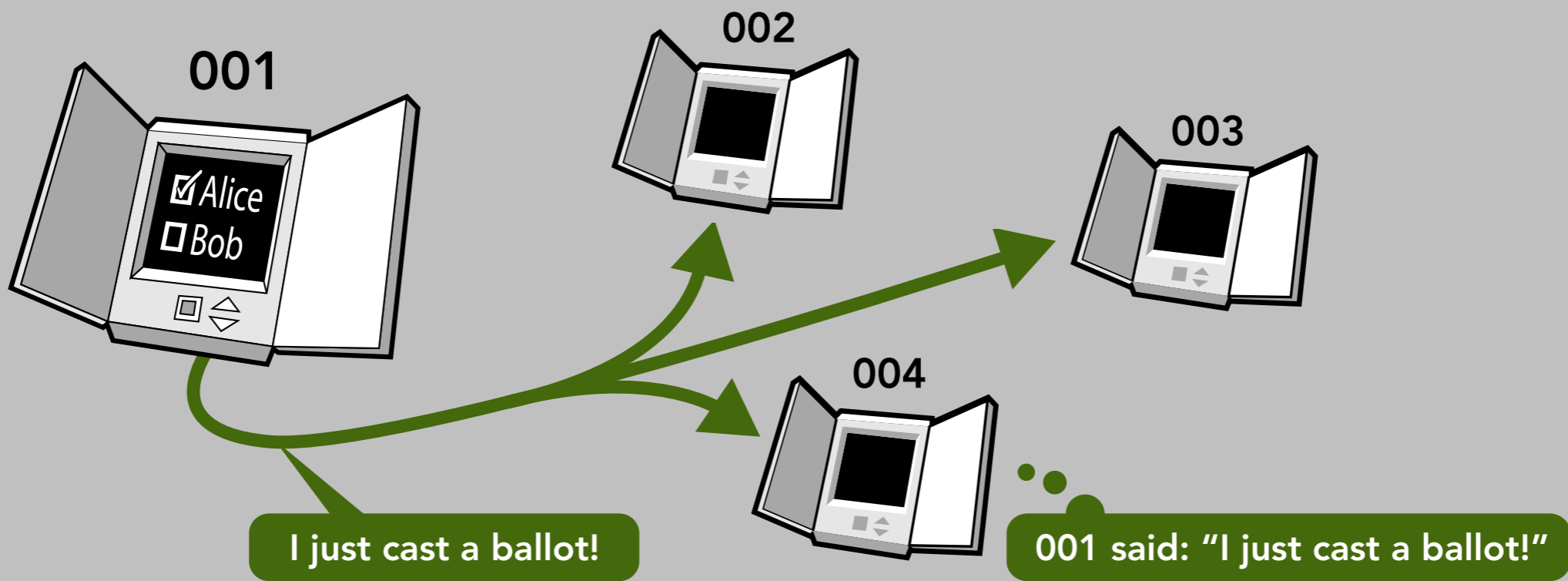
# Ingredient #3: Broadcast

## **All-to-all communication**

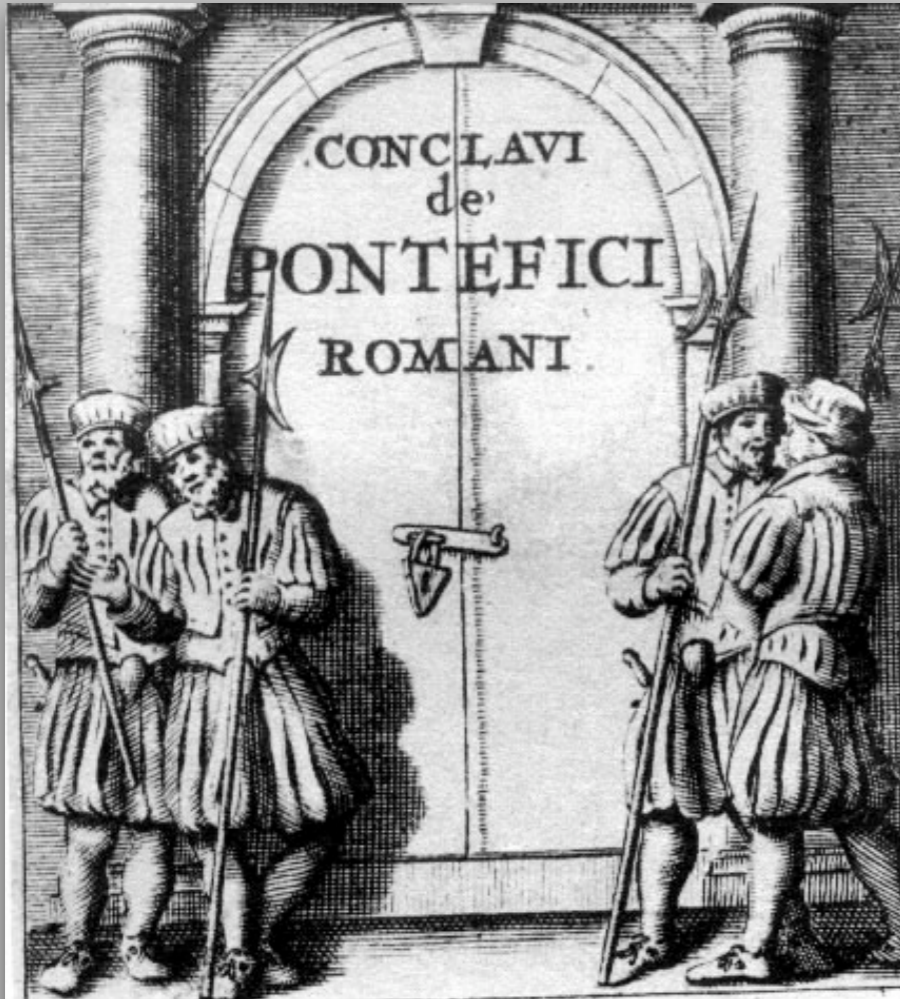
Allows entanglement

Widespread replication

Broadcast entanglement =  
**Auditorium**



Everyone hears everything in the Auditorium.



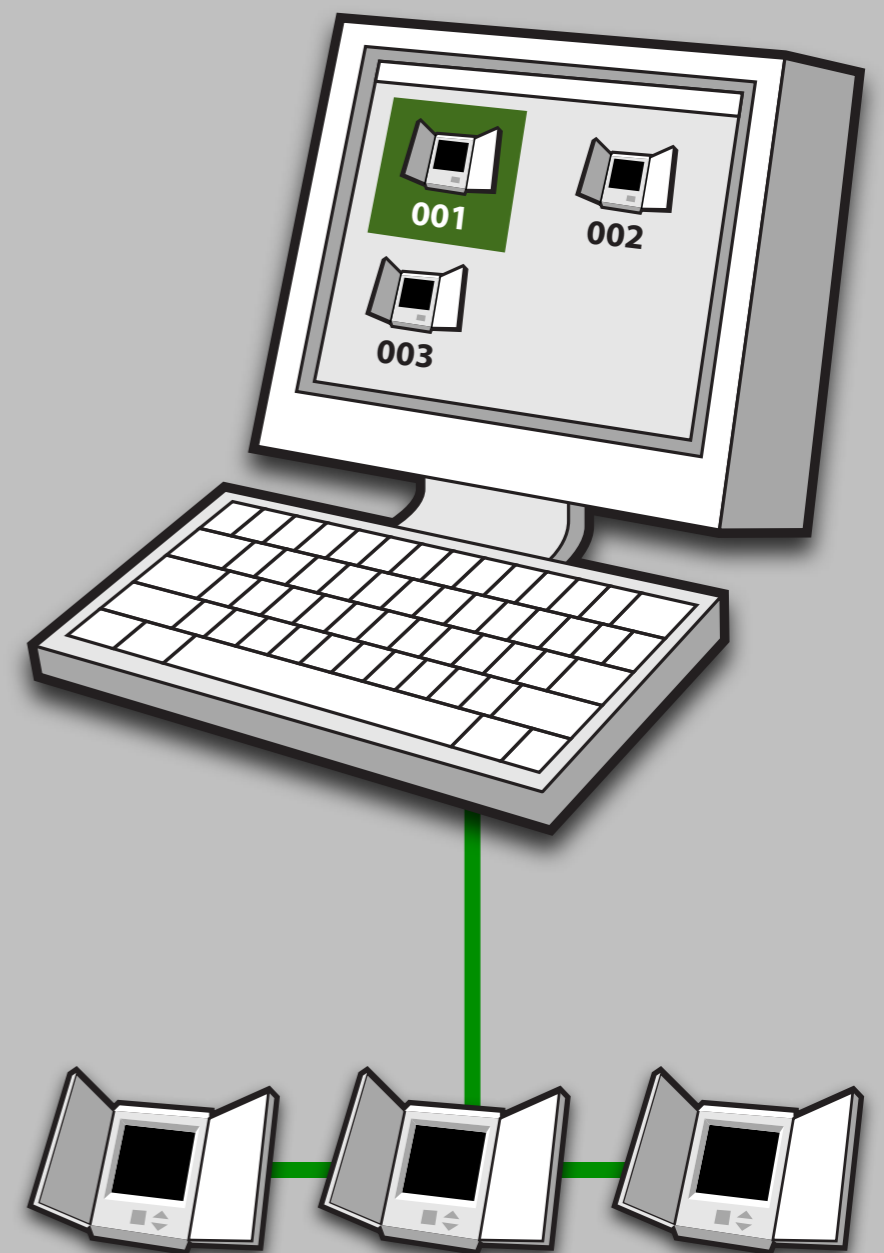
## The Papal Conclave

Proceedings closed to outsiders

All ballots cast in plain view

All ballots secret

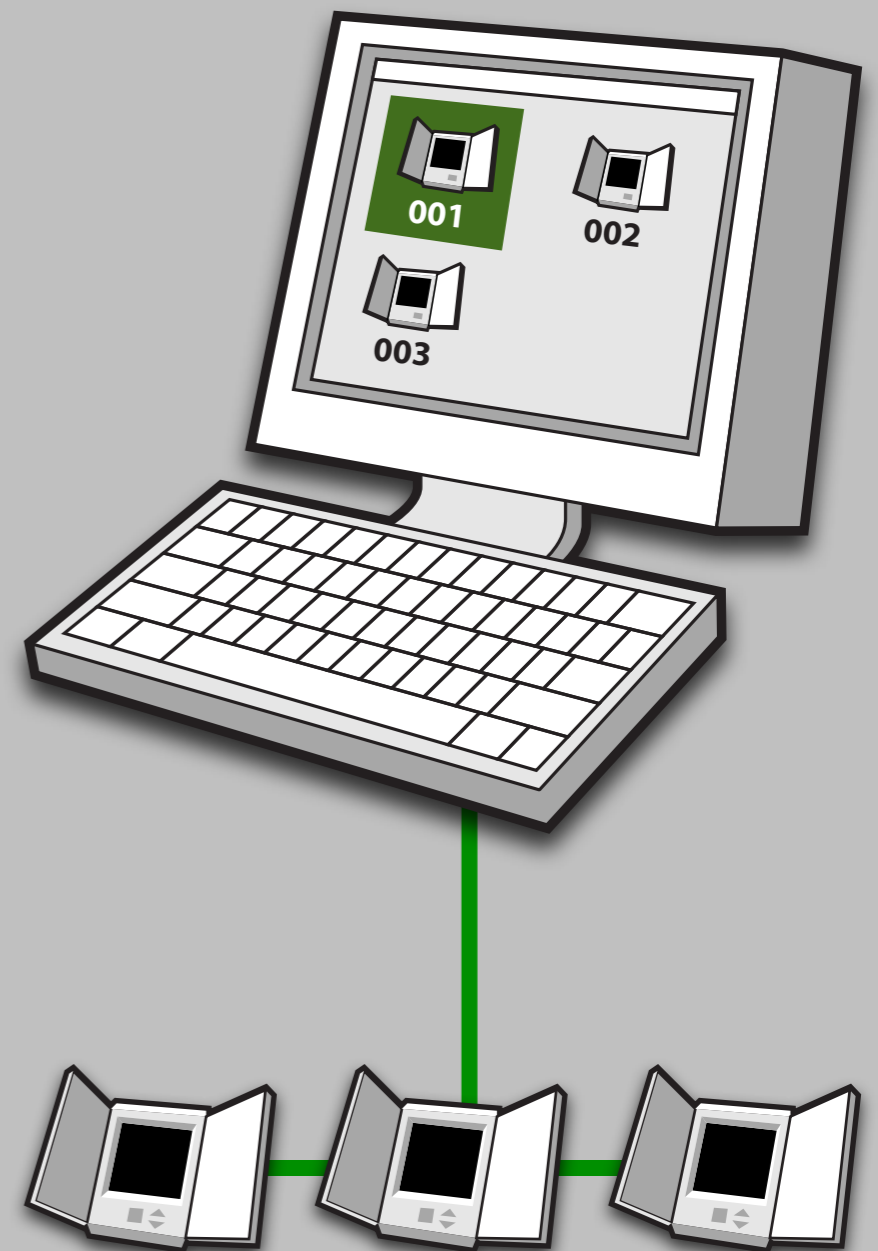
# The supervisor console



# The supervisor console

**Shows status of all machines**

Votes cast, battery running low, etc.



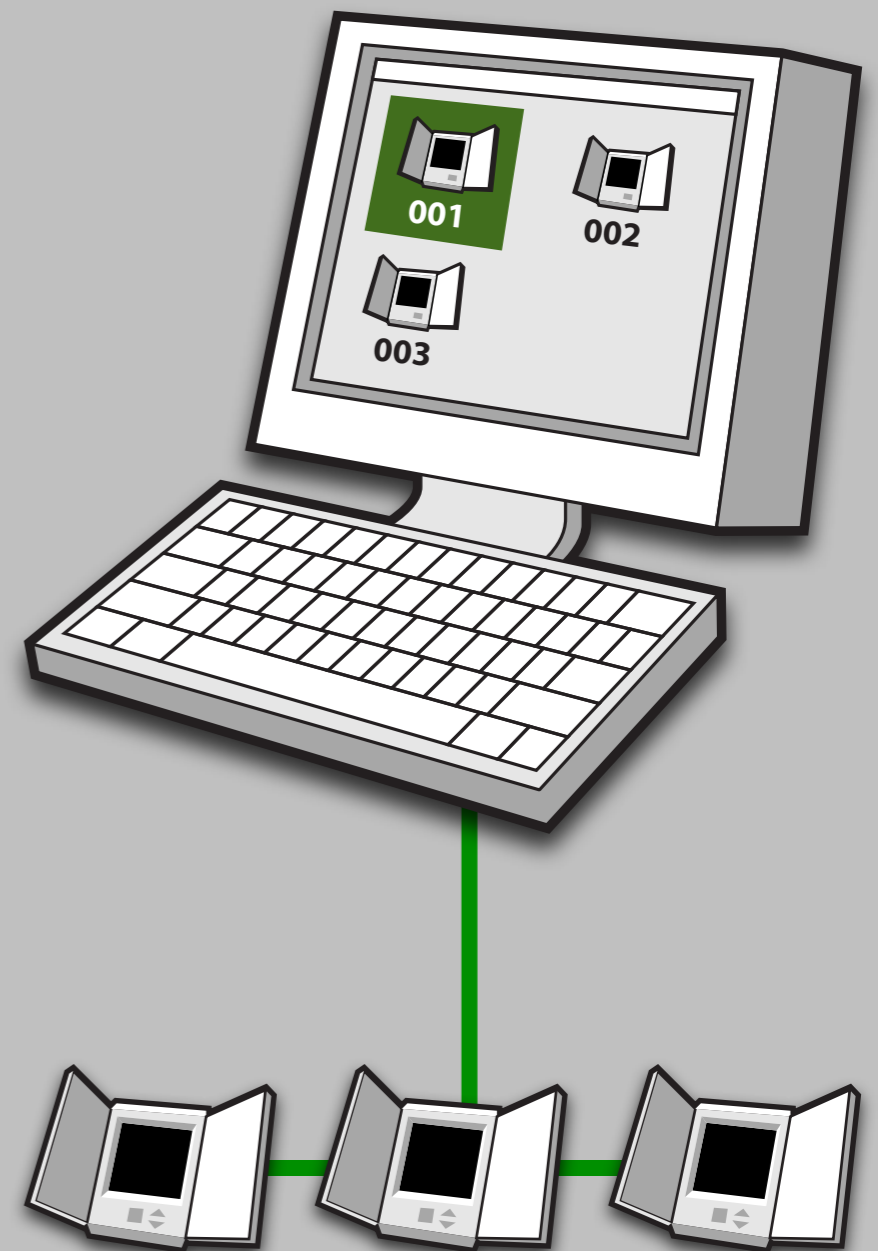
# The supervisor console

## Shows status of all machines

Votes cast, battery running low, etc.

## Helps conduct the election

Less opportunity for poll-worker error



# The supervisor console

## Shows status of all machines

Votes cast, battery running low, etc.

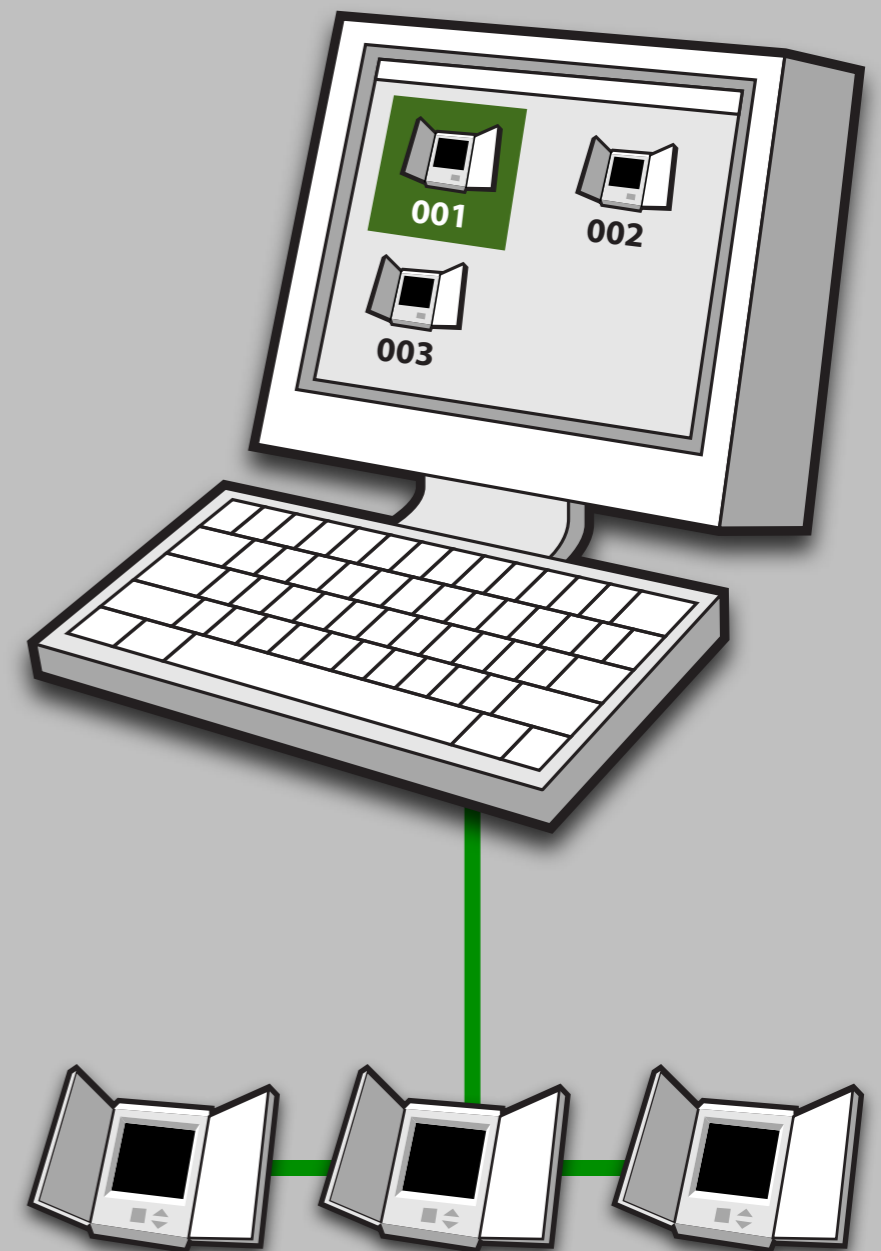
## Helps conduct the election

Less opportunity for poll-worker error

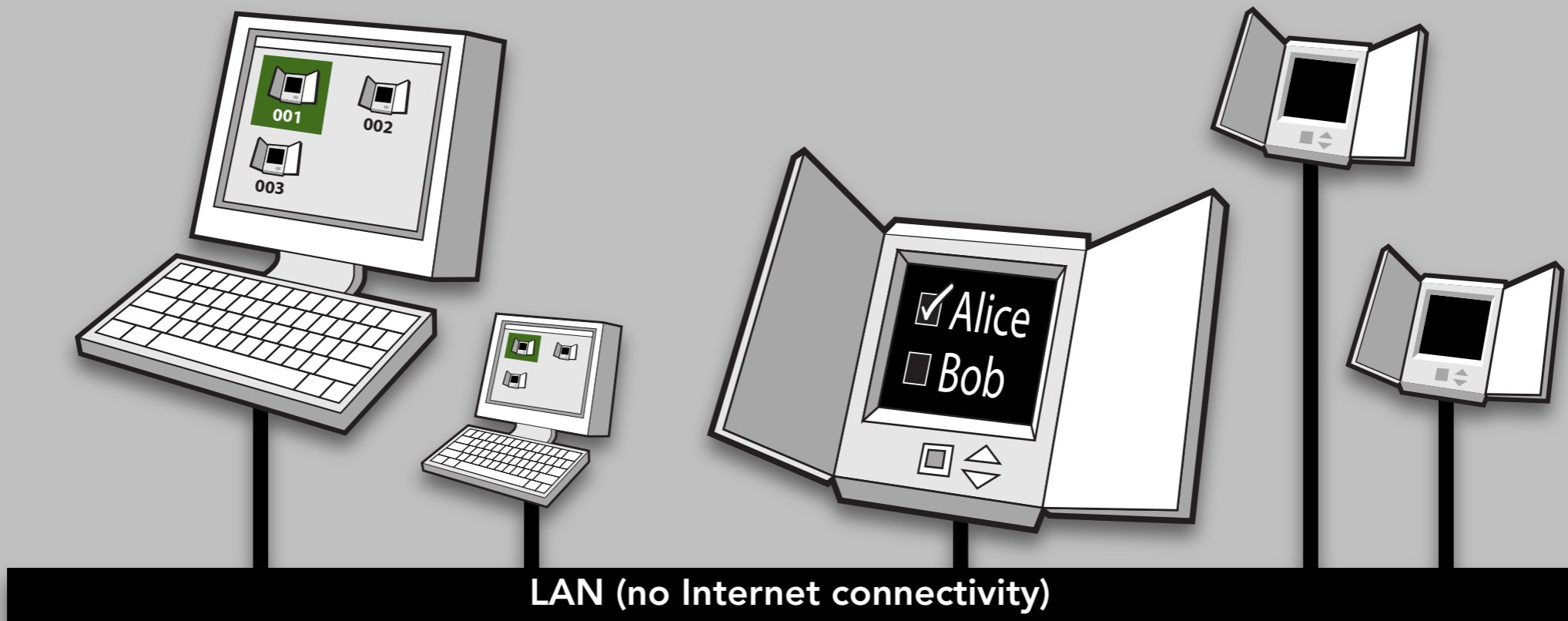
## Ballots distributed over the network

Booths are stateless, interchangeable

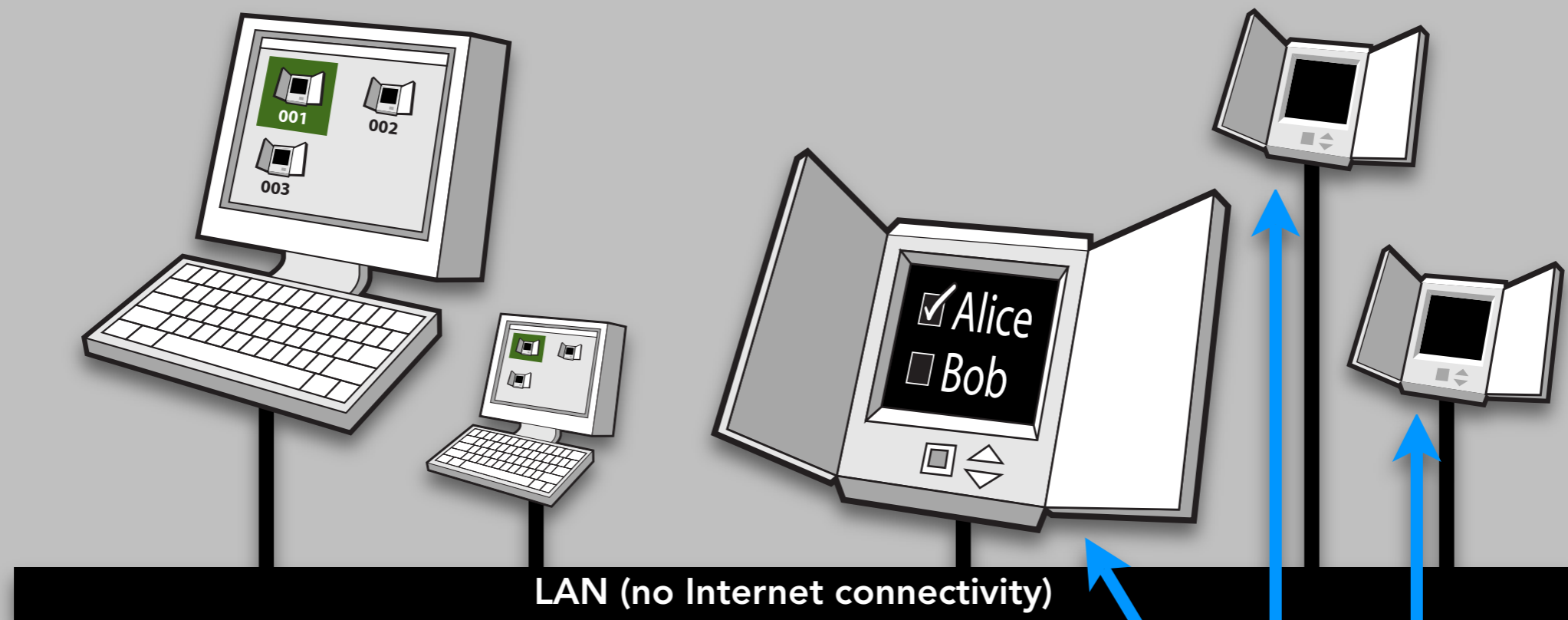
Supervisor has a hot spare, too



# Voting in the Auditorium



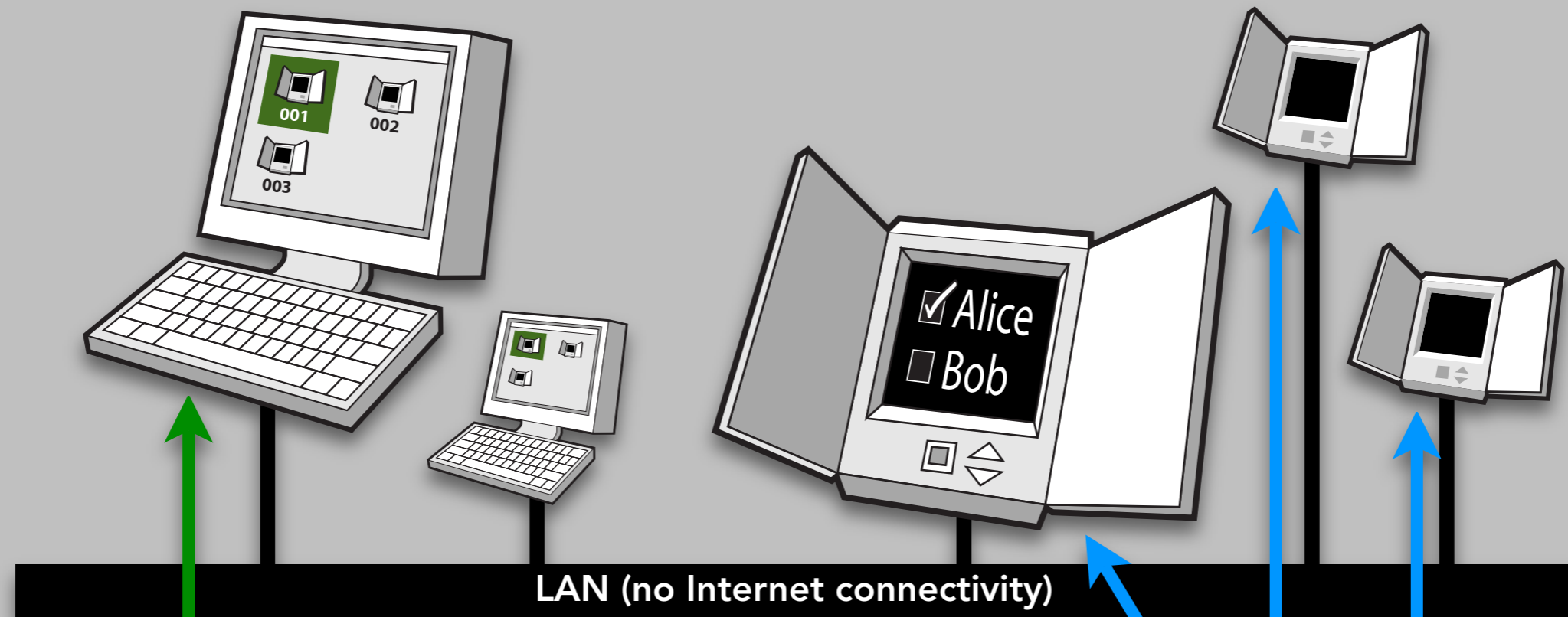
# Voting in the Auditorium



## BOOTHS

Listen for vote authorizations (ballots)  
Capture voter selections  
**Broadcast** encrypted votes  
Record all broadcast messages

# Voting in the Auditorium



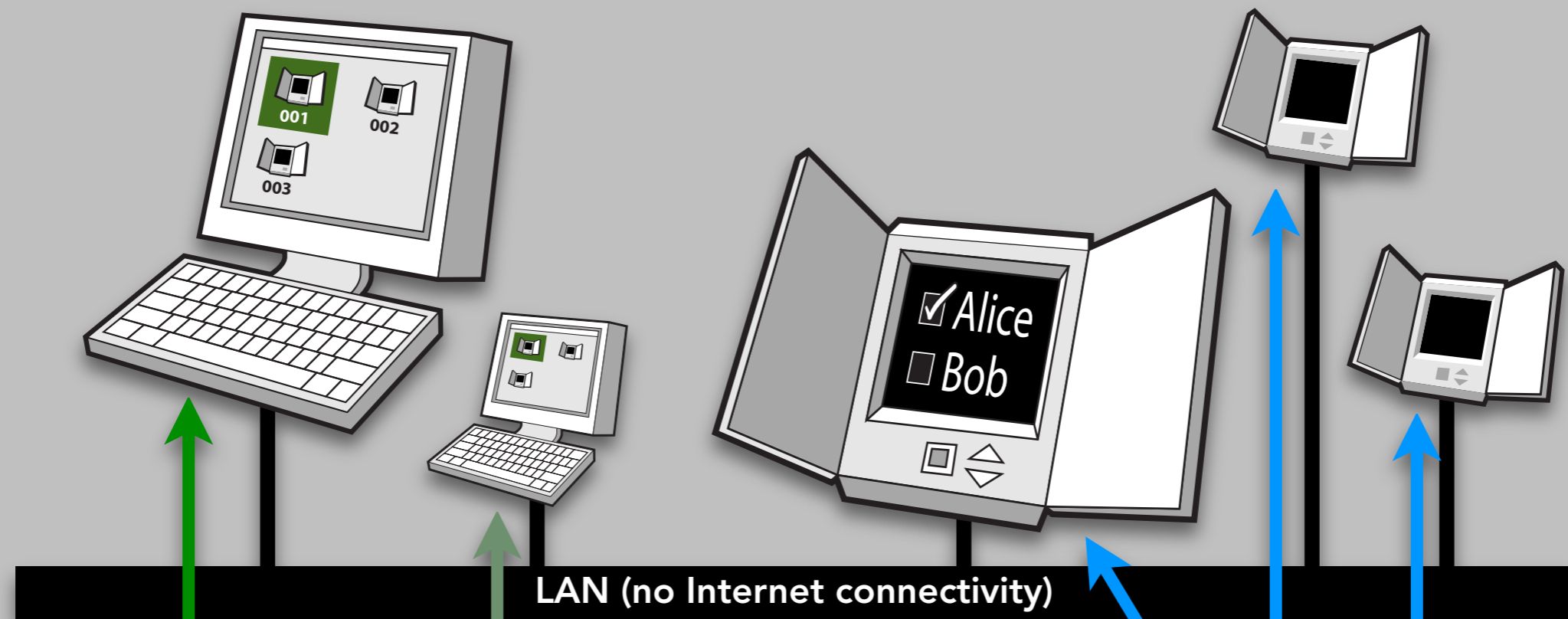
## SUPERVISOR

Monitors, displays booth status  
**Broadcasts** vote authorizations  
Records all broadcast messages

## BOOTHS

Listen for vote authorizations (ballots)  
Capture voter selections  
**Broadcast** encrypted votes  
Record all broadcast messages

# Voting in the Auditorium



## SUPERVISOR

Monitors, displays booth status  
**Broadcasts** vote authorizations  
*Records all broadcast messages*

## SUPERVISOR (BACKUP)

Ready to assume supervisor's  
responsibilities at any time  
*Records all broadcast messages*

## BOOTHS

Listen for vote authorizations (ballots)  
Capture voter selections  
**Broadcast** encrypted votes  
*Record all broadcast messages*

# Attacks

# Attacks (1)

## Early machine exit (e.g. equipment failure)

*Votes safely replicated on other machines*

*Votes provably legit (authorized by supervisor, etc)*

## Late machine entry

*Cleared? See above.*

*Hot spare? Logs prove the machine hasn't been used.*

# Attacks (2)

## Ballots cast on the wrong day

Clock set wrong? *Hash chain OK; votes legit*

Test votes? *No hash chain connection to poll opening.*

## Intentional subversion

Stuffed ballots? *Like test votes: invalid.*

Removed ballots? *Provably missing from hash chain.*

# Mega attacks

# Switched results

# Switched results

## Scenario

Malicious parties in control of precinct

Day before election: attackers conduct a **secret election**

Swap those results for the election day results

Secret election could also be *post facto*

# Switched results

## Scenario

Malicious parties in control of precinct

Day before election: attackers conduct a **secret election**

Swap those results for the election day results

Secret election could also be *post facto*

## Countermeasures?

Election start nonce ("launch code") — added to (polls-open)

Quickly publish hash of final (polls-closed) event

# Concurrent shadow election

# Concurrent shadow election

## Scenario

Malicious parties create duplicate precinct

On election day, conduct secret election using appropriate start nonce

# Concurrent shadow election

## Scenario

Malicious parties create duplicate precinct

On election day, conduct secret election using appropriate start nonce

## Countermeasures?

TPM to resist duplication of booth key material (signed by high-ranking election officials)

# Booth capture

# Booth capture

## Scenario

Armed attackers take control of the polling place by force and stuff ballots—or destroy them—until the police arrive

# Booth capture

## Scenario

Armed attackers take control of the polling place by force and stuff ballots—or destroy them—until the police arrive

## Detection

Trivial

# Booth capture

## Scenario

Armed attackers take control of the polling place by force and stuff ballots—or destroy them—until the police arrive

## Detection

Trivial

## Countermeasures?

Partial destruction is recoverable from intact machines

# Software tampering

# Software tampering

## Scenario

Malicious software

Introduced by poll workers, voters, "field upgrades"

# Software tampering

## Scenario

Malicious software

Introduced by poll workers, voters, “field upgrades”

## Countermeasures

TPM, other orthogonal approaches

Lots of current research

# Conclusion

**In real elections...**

# In real elections...

Mistakes are made

# In real elections...

Mistakes are made

Data is lost

# In real elections...

Mistakes are made

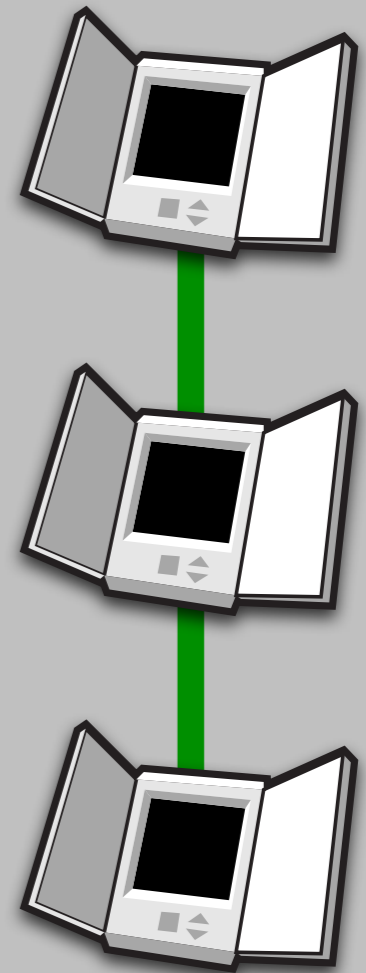
Data is lost

**Auditing is...challenging**



# Auditorium

an *auditable* record of election day

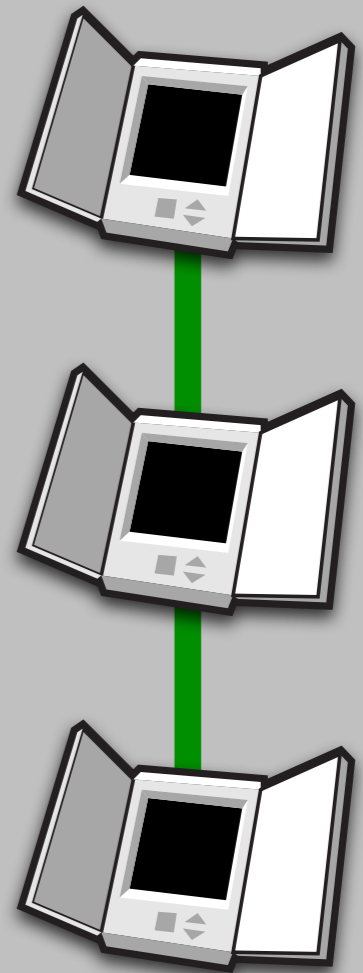


# Auditorium

an *auditable* record of election day

**All election events linked in a secure timeline**

No ambiguity about when a vote was cast



# Auditorium

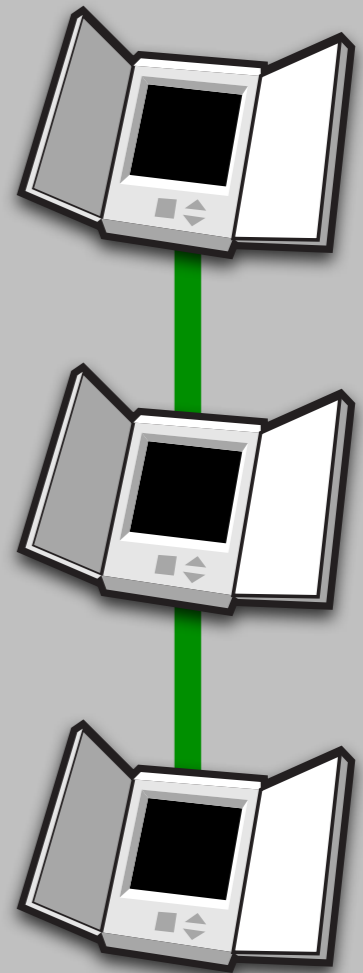
an *auditable* record of election day

**All election events linked in a secure timeline**

No ambiguity about when a vote was cast

**Entanglement + broadcast = recoverability**

A lost machine's votes are safe and believable



# Auditorium

*an auditable record of election day*

**All election events linked in a secure timeline**

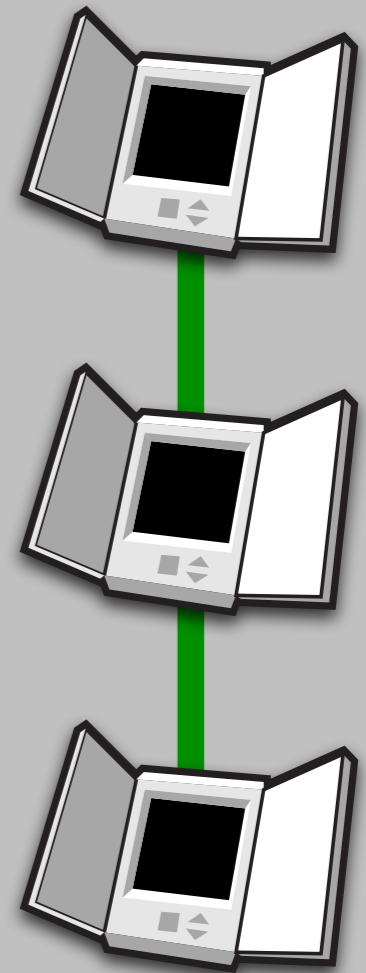
No ambiguity about when a vote was cast

**Entanglement + broadcast = recoverability**

A lost machine's votes are safe and believable

**Composable with other secure e-voting ideas**

VVPAT, secure vote storage, trusted computing



# Auditorium

an *auditable* record of election day

**All election events linked in a secure timeline**

No ambiguity about when a vote was cast

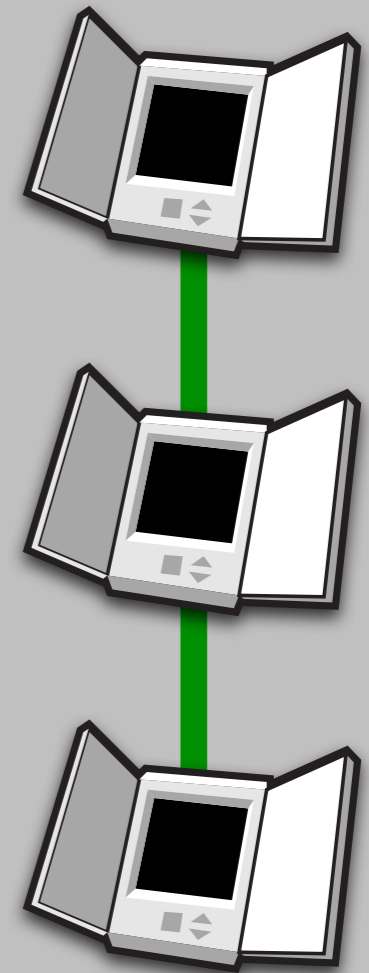
**Entanglement + broadcast = recoverability**

A lost machine's votes are safe and believable

**Composable with other secure e-voting ideas**

VVPAT, secure vote storage, trusted computing

**Don't fear the (air-gapped) network!**



# thanks

## **VoteBox team**

Kyle Derr, Corey Shaw, Ted Torous

## **Rice Computer-Human Interaction Lab**

Mike Byrne, Sarah Everett, Kristen Greene

**NSF/ACCURATE**



*fin*