Electronic Voting

Aggelos Kiayias

E-voting in Greece

“Είμαι της άποψης ότι η χρήση τεχνολογίας να μπει στη ζωή μας, αλλά αν είναι έτσι να καταργήσουμε τα παραβάν κλπ και τότε να ψηφίζουμε όλοι από το λαπ τοπ μας. Με την ηλεκτρονική ψηφοφορία αφήνονται τα ηλεκτρονικά ίχνη, μπορεί να είναι στη διάθεση κάθε ενδιαφερόμενου, δεν διασφαλίζεται το απόρρητο. Δεν υπάρχει κάποιος να μετρά τους ψήφους, αλλά ένας σερβερ. “

Prime Minister Tsipras, 8/5/2015

E2E Voting DEMOS

- Created in 2014-2015 at the U. Athens.
- Joint work T. Zacharias, B. Zhang.
- slides credit : T. Zacharias

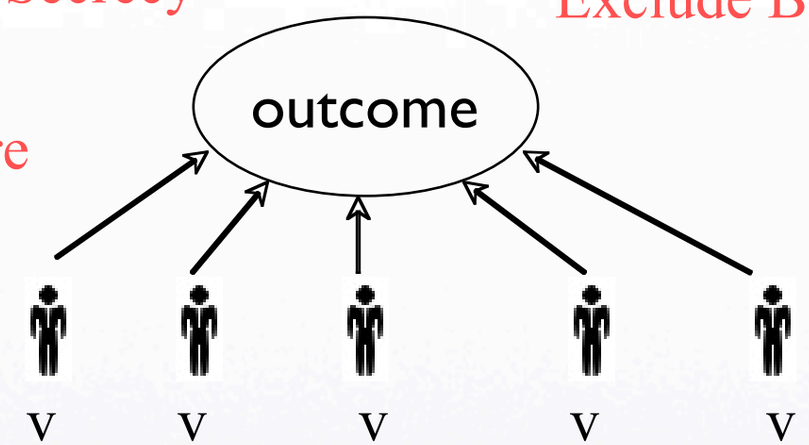
Electronic Voting

Authorities:

Violate Ballot Secrecy

Exclude Ballots from Tally

Untimely Disclosure
of partial tallies



Voters:

Disrupt the protocol (maliciously or not)

Double-Voting

Obtain Receipts
revealing how they voted

Properties

- Robustness/ Fault Tolerance
- Auditability
- Ballot Secrecy
- Enforcement of voter eligibility
- Receipt-freeness
- Trust distribution
- "Vote-and-go"
- Dispute-freeness
- Fairness

Two Paradigms

- Remote voting
- Onsite voting

Remote voting

- Precinct ballot casting and tabulation process physically separated.
- Ballot casting is facilitated by (at least partially) untrusted environment.

Bulletin Board approach

Bulletin Board

Voter	Choice
V_1	(candidate B)
V_2	(candidate C)
V_3	(candidate A)
V_4	(candidate A)

A useful abstraction

1. Access Control.
2. Authenticated `read` operation.
3. Authenticated `append` operation.

Provides : voter eligibility, verifiability, auditability.

Summing & Voting

Example

Suppose we have four voters:

Voter	Choice
V_1	0 (no)
V_2	1 (yes)
V_3	1 (yes)
V_4	1 (yes)

When the votes are tabulated, the result is $0 + 1 + 1 + 1 = 3$, which gives us the number of 'yes' votes. This, subtracted from the total number of votes, gives $4 - 3 = 1$, which is the number of 'no' votes.

Summing & Voting

Example

Imagine a three-way election, and four voters:

Voter	Choice
V_1	010 (candidate B)
V_2	100 (candidate C)
V_3	001 (candidate A)
V_4	001 (candidate A)

Tabulation is base-M addition, where M is greater than the number of voters. The result is $010 + 100 + 001 + 001 = 112$. Each position gives us the number of votes for each candidate: 2 for A, 1 for B, and 1 for C. A is the winner.

Privacy in Bulletin Board Voting

- Voters encrypt their votes using special purpose encryption that:
  - has the following *homomorphic* property:

$$\mathcal{E}(x_1) \odot \mathcal{E}(x_2) = \mathcal{E}(x_1 + x_2 \bmod q)$$

Issues

- Key Management
- Trust Distribution
- Fault Tolerance
- Client Misbehavior

Issues Addressed

- Key Management *Threshold Cryptography*
- Trust Distribution *Threshold Cryptography*
- Fault Tolerance *Threshold Cryptography*
- Client Misbehavior *Zero-knowledge proofs*

Threshold Cryptography

Desmedt '87

- Like regular cryptography but keys are controlled by body of entities and a quorum is needed to apply the key.
- Need to design protocols for each operation (e.g., key-generation, decryption for the case of a public-key cryptosystem).

Additive Secret Sharing

shares $x_1, \ldots, x_n \in \{0,1\}^n$

secret $s \in \{0,1\}^n$

Select $x_1, \ldots, x_{n-1}$ at random

Set $x_n = x_1 \oplus \ldots \oplus x_{n-1} \oplus s$

Observe $\oplus_{i=1}^{n} x_i = s$

but any n-1 size subset of $x_1, \ldots, x_n$ reveals no info

Shamir's Secret-Sharing

Suppose is a polynomial $P(x)$ of degree $n-1$. This polynomial can be expressed in two ways:

1. **Coefficient form**: $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$.
2. **Point-value form**: $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$.

We can convert from point-value form to coefficient form (and thus evaluate $P(x)$ at arbitrary points), provided we have n distinct points, using the following formula:

$$P(x) = \sum_{j=1}^{n} P_j(x), \qquad P_j(x) = y_j \prod_{\substack{k=1 \\ k \neq j}}^{n} \frac{x - x_k}{x_j - x_k}.$$

Secret-Sharing

- Say we have a secret S that we wish to distribute, with a threshold of n. We can create a polynomial of degree $n-1$:

$$P(x) = S + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1},$$

  and distribute the values $P(x_1), P(x_2), P(x_3), \ldots$
- To reconstruct S, n shares must be combined, and the interpolation formula used to evaluate $P(0)$.
- It is *impossible* to recover the polynomial without n points, so the secret is safe without n shares.
- If a few shares are missing, the operation will still work, as we can use *any* n points.

Problem:

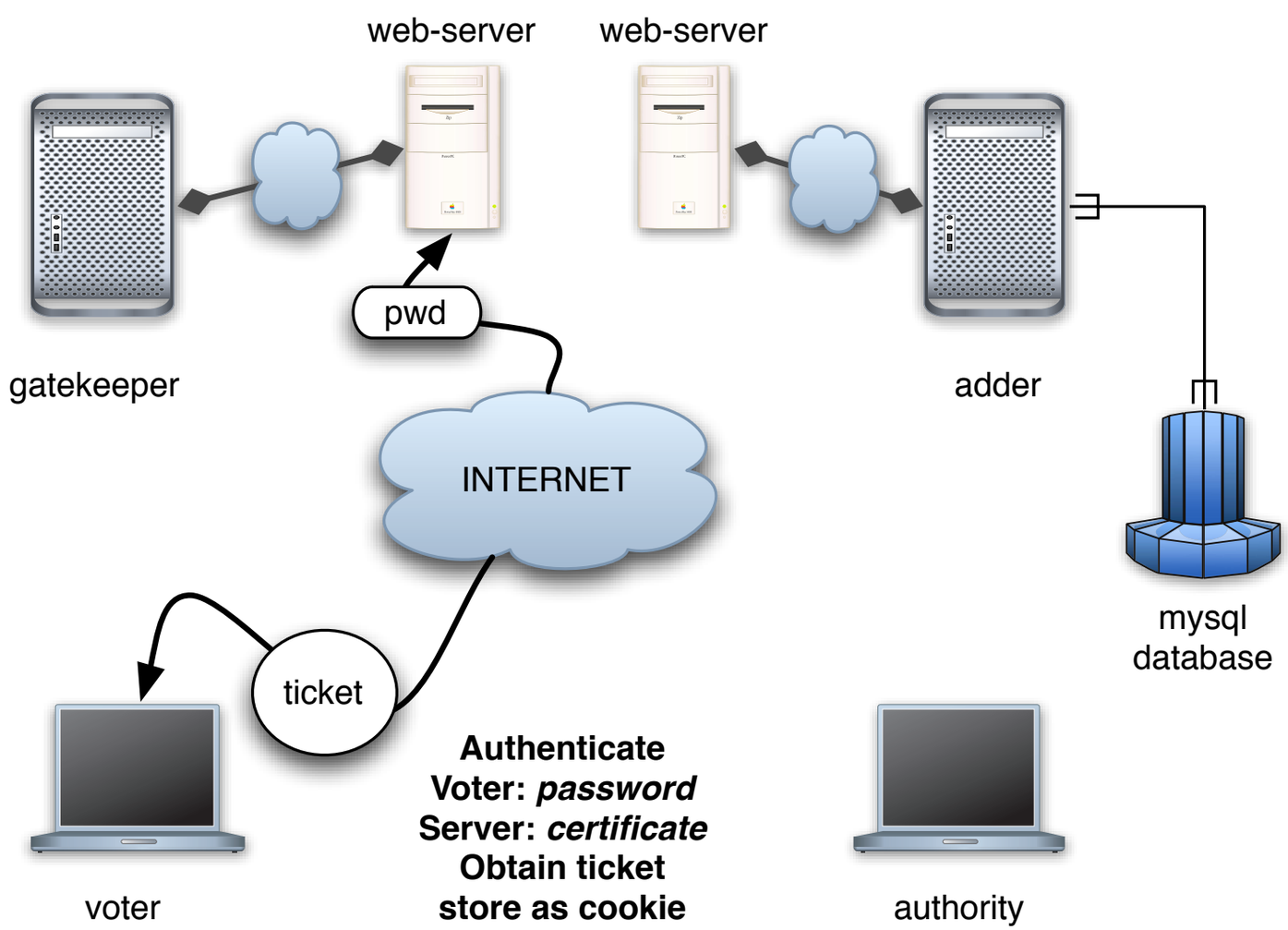
- Who is going to "deal" the shares?
- Solution: parties may simulate the dealer on their own!

Adder System

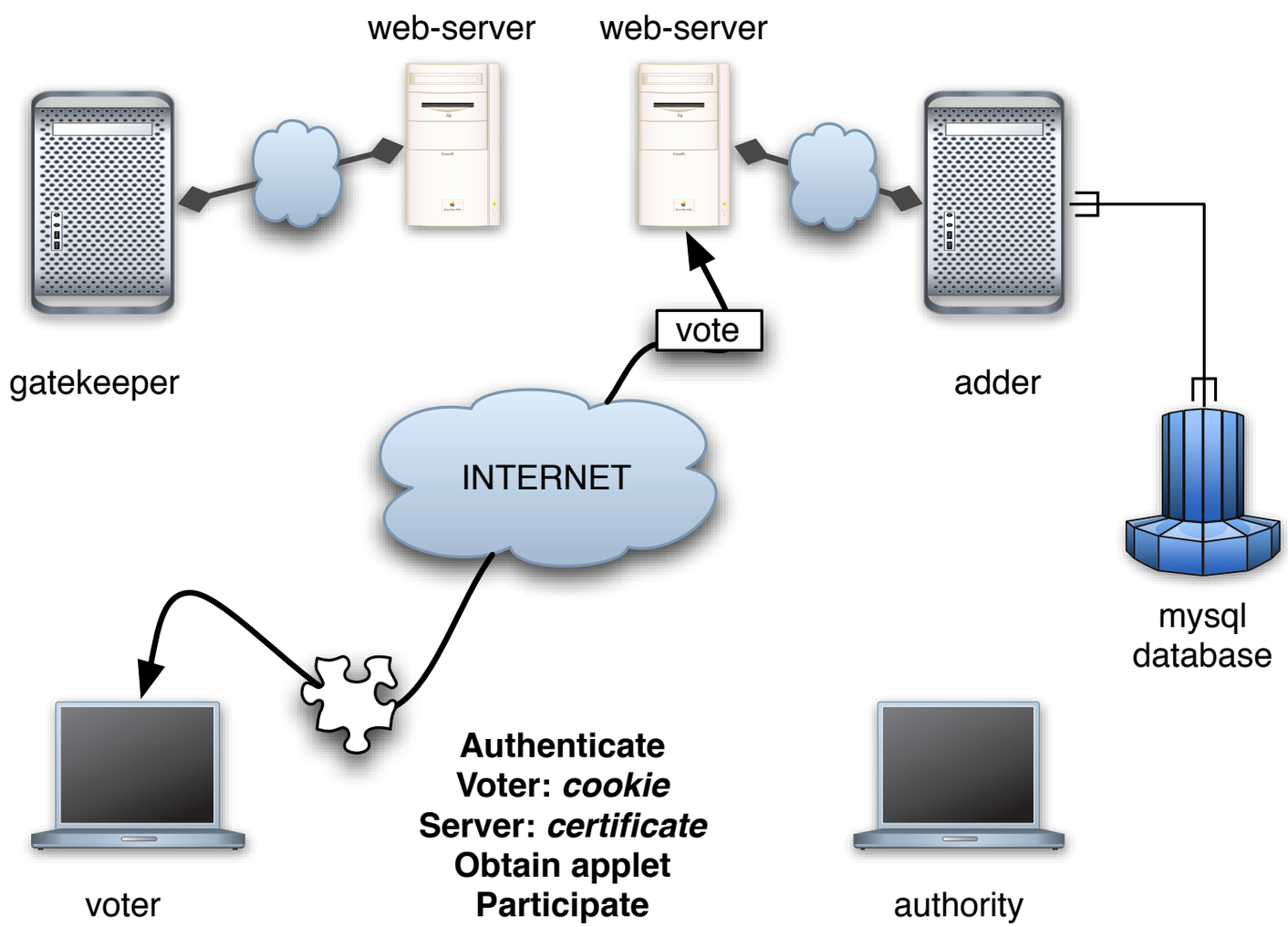
An Internet Voting System Supporting User Privacy.
Kiayias, Korman, Walluck, ACSAC 2006

- Implements all the above in a web-based environment.
- uses: Java or C++ on client-side. PHP, C++ with MySQL on server side.
- Released under GPL

Adder, I


web-server
web-server
gatekeeper
adder
pwd
INTERNET
mysql
database
ticket
Authenticate
Voter: *password*
Server: *certificate*
Obtain ticket
store as cookie
voter
authority

Adder, II


web-server
web-server
gatekeeper
vote
adder
INTERNET
mysql
database
Authenticate
Voter: *cookie*
Server: *certificate*
Obtain applet
Participate
voter
authority

Problems of Remote Voting

- Voter Coercion
- Network security concerns:
  - Denial of Service (Tabulation server open to outside connections).
  - Viruses that switch/steal/record your vote (Untrusted ballot-casting environment).

National Elections

- Is remote voting a good idea?
  - facilitates absentee ballot casting.
- but ...
- Is electronic voting a good idea??

Advantages of E-voting

- eliminating/reducing overvoting and undervoting.
- flexible interface
- accessibility for disabled citizens
- many languages
- automatic tabulation / smaller errors

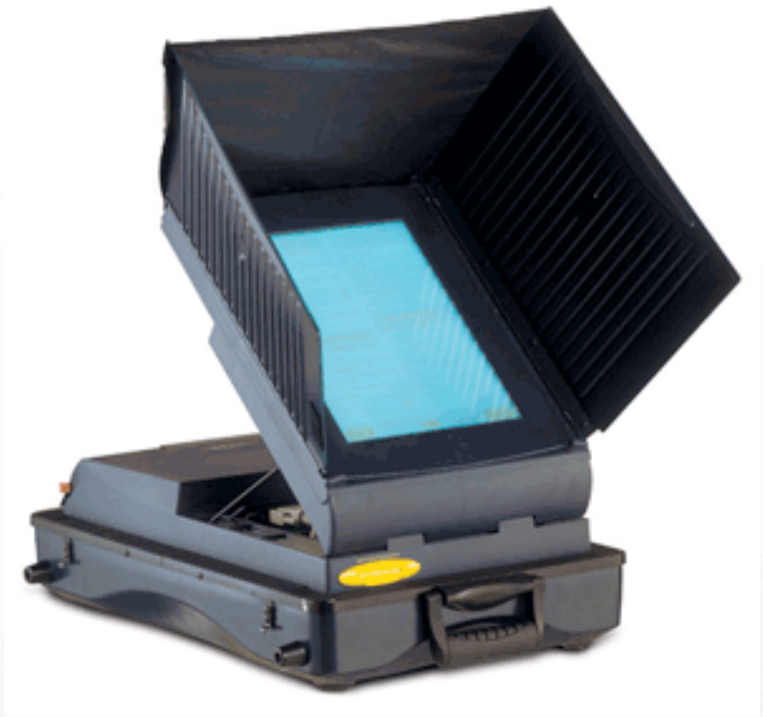
Voting Machine Lifetime

- Long term warehouse storage.
- Election HQ (county).
- Transportation to Poll sites.
- Temporary storage (”sleepovers”)
- Prime time!
- Termination.
- Reporting back to Election HQ.
- Back to storage.

Equipment

Diebold Accuvote TS

Avante VoteTrakker



Sequoia

Issues

- Modify election results.
- Violate the privacy of the voter.
- Disrupt the election process.
- Voting receipts & Coercion.
- Inaccurate audit-trail (if it exists!)
- Bias results through interface manipulation.

Bootstrapping Vulnerabilities

- E-voting system must employ trusted computing techniques.
- Tampering with the boot process is catastrophic for elections.

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 problem may be hard (a bad design choice), and even if it is easy, decision test may not be properly implemented).
- Cryptographic integrity checking?
  - 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)

Configuration Vulnerabilities

- Obvious reset / power buttons.
- Sequential paper trail.
- Hard to verify that only a single VVAT record is printed.
- example : The VT should never be in a state where a voter can obtain a receipt by taking a picture.

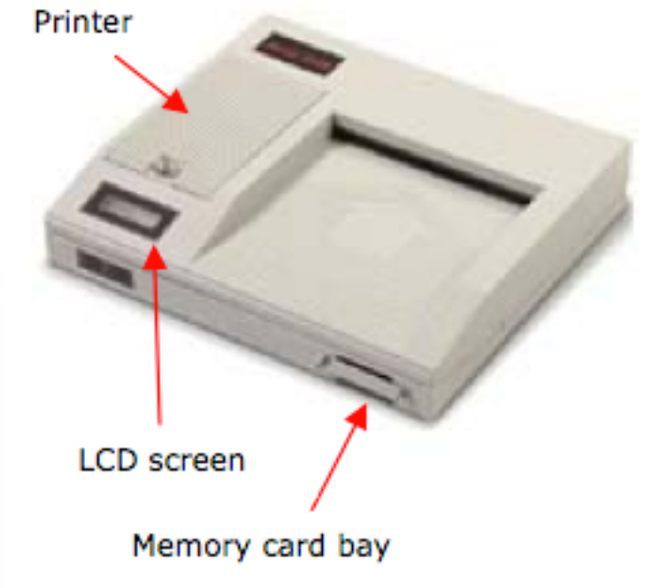
Tabulation Vulnerabilities

- VT impersonation during the post-election stage of transferring results to the CTS.
- Aggregation vulnerabilities: CTS vulnerability when pooling results together.

Case Study I

- H. Hursti; BlackBox Voting.
  - http://www.blackboxvoting.org/BBVreport.pdf
    - Accuvote Optical Scan

Attack Vector



- Prior to election the memory card of a VT is compromised.
- Memory card contains byte code + counters.

Attack Vector, II

- Byte code is used for reporting functionalities.
  - can be modified to report that the counters are 0-ed (even though they are not).
- There is no integer overflow exception:
  - the 16-bit counters can be initialized to values like 65530.
- No (cryptographic) integrity check performed.

Threat Assessment

- A poll-worker with access to the machine in a pre-election stage could substitute the memory card with a properly programmed one.
- If this is accomplished the election will appear to run smoothly throughout but the results will be wrong.
- A mock election performed in Leon County, FL confirmed the above.

Case Study II

- Feldman, Halderman, Felten.
  - http://itpolicy.princeton.edu/voting/ts-paper.pdf

The attack vector exploits a bootstrapping vulnerability

TS Voting Terminal

Possibility of Virus

- Diebold TS VT is a Windows CE system.
- Tampering with the bootstrapping process introduces a modified kernel that is capable of possibly replicating itself when a memory card is moved from one machine to the next.

Case Study III

UConn VoTeR Center

Kiayias, Michel, Russell, Shvartsman

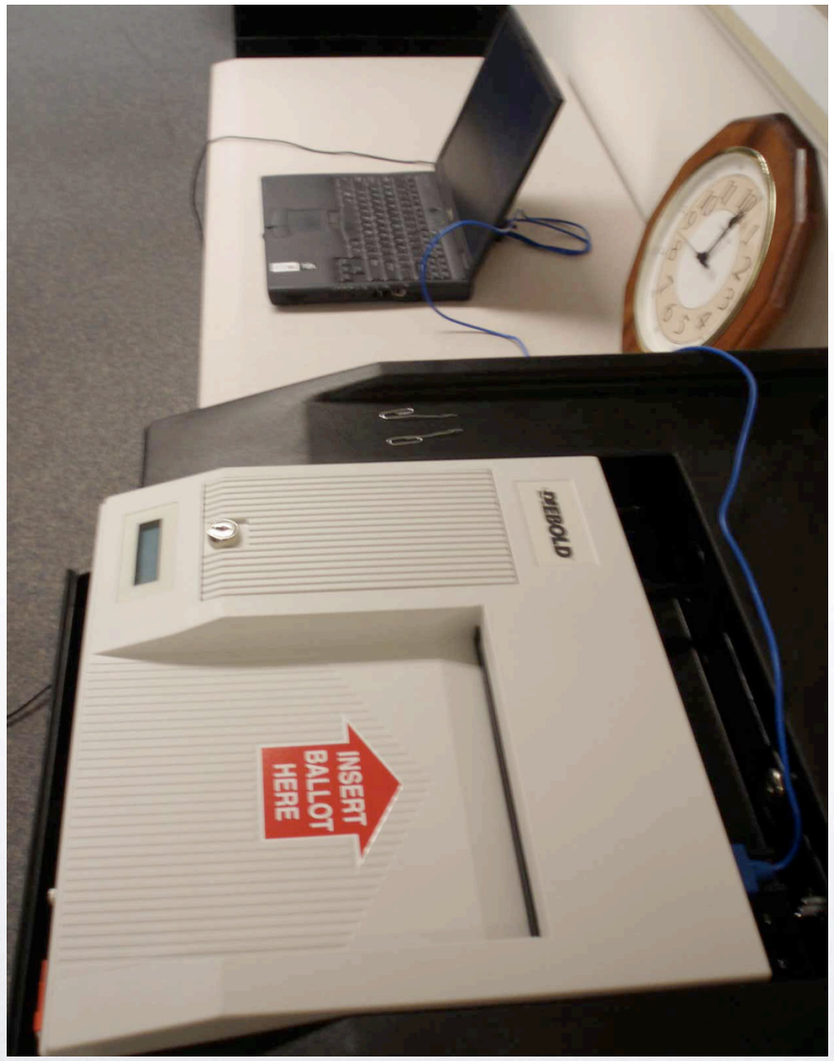
Accuvote Optical Scanner used in all CT elections

Hacking the machine in minutes

- Exploits vulnerability in authentication between voting terminal and central tabulation system.
- The machine has no way of knowing who is the one it talks to.
- Attacker needs to get access to serial port + administrator password.

Freeing the machine

Our setup



serial
connection

Dumping memory contents

card is sealed inside the system

cards contents are dumped by the terminal when in diagnostic mode.

password is stored into card.

Differential Protocol Analysis

- We observed various card contents using different PINs.
- Using this information we cracked the password storage mechanism.

Attacker's front-end

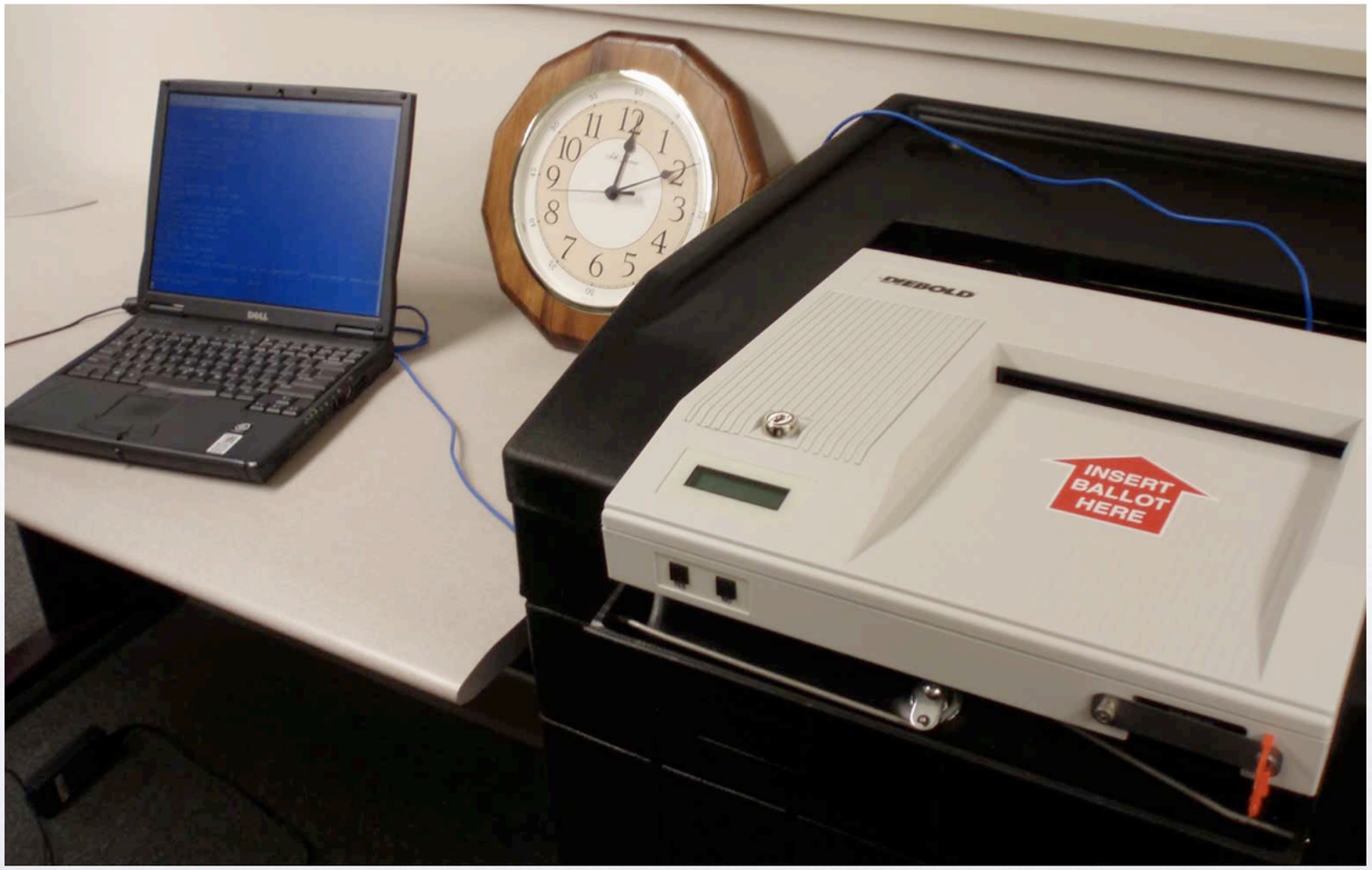
```
PIN:7251
Location:WESTPORT, CONN.
Election:MUNICIPAL ELECTION
Options:
(1) Neutralize candidate votes
(2) Swap candidates votes
(C) Print candidate list
(D) Display election info
(Q) Quit and send data
Choice:c
                        name     Bubble position(x,y)
BOARD OF FINANCE:
          R.GAVIN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

Burning the card

Attacker gets access to supervisor mode

Machine obliges

End of compromise



Attack Payload

- Swapped candidates by messing with bubble-sheet layout as encoded within the system.
- Machine is a time-bomb: attack will only get active when the right time comes.
- Running a mock election will NOT detect the attack!

Attack Prevention

- Seal the serial ports.
- Unbroken Chain of custody.
- *Hopefully in the future:* voting terminal manufacturers will consult with people that understand security.

Read more

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