<table>
<thead>
<tr>
<th>State</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governor</td>
<td>Governor</td>
</tr>
<tr>
<td>Amelia Earhart</td>
<td>Amelia Earhart</td>
</tr>
<tr>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□</td>
<td>✗</td>
</tr>
<tr>
<td>Howard Hughes</td>
<td>Howard Hughes</td>
</tr>
<tr>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□</td>
<td></td>
</tr>
<tr>
<td>Charles Lindbergh</td>
<td>Charles Lindbergh</td>
</tr>
<tr>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□</td>
<td></td>
</tr>
<tr>
<td>Write In</td>
<td>Write In</td>
</tr>
<tr>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>□</td>
<td></td>
</tr>
</tbody>
</table>

**UNCLEARBALLOT: AUTOMATED BALLOT IMAGE MANIPULATION**

Jeremy Wink  Kartikeya Kandula

jeremy@umich.edu  kartkand@umich.edu

University of Michigan

Joint work with Matthew Bernhard

and Professor J. Alex Halderman
Post-Election Audits

- Audits are one of the most important layers of defense for election security
- Risk-limiting audits: manually inspect large enough random sample of physical paper ballots – considered gold standard
- Other types of post-election audits are gaining popularity in the marketplace
- 37 states along with DC require post-election audits of ballots
Image Audits

- Audit of digital scan rather than physical paper
- Image audit software pioneered by Clear Ballot
- Maryland relies on image audits to provide assurances of election results
  - codified into election code
- Images are disconnected from source of truth—physical paper ballots
  - Not reliable under adversarial conditions
Attack Scenarios

- We investigate how an attacker could automatically alter ballot images to change apparent votes
- Numerous vulnerabilities documented to allow attacker to infect voting equipment and change tabulation results
- Our attack targets a tabulation machine and manipulates each ballot as it is scanned
Our approach: automatically and selectively doctor ballot scans
- altered marks consistent with voter’s marks
- undetectable to human eye
- not necessary to alter large proportion
Template Matching: Identify Race
Hough Line Transforms: Separate candidates

For US Senator
(Vote for not more than 1)

Jonathan Hart
Democratic

Adam Martin
Republican

George Smith
Green

Write-In

For US Senator
(Vote for not more than 1)

Adam Martin
Republican

George Smith
Green

Write-In
Vertical Sweep: Remove race title
Linear Sweeps:
Create bounding box

- Four linear sweeps
- Taking pixel intensity
Identify and move the mark
Example swaps

<table>
<thead>
<tr>
<th>State</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governor</td>
<td>Governor</td>
</tr>
<tr>
<td>Amelia Earhart</td>
<td>Amelia Earhart</td>
</tr>
<tr>
<td>Howard Hughes</td>
<td>Howard Hughes</td>
</tr>
<tr>
<td>Charles Lindbergh</td>
<td>Charles Lindbergh</td>
</tr>
<tr>
<td>Write In</td>
<td>Write In</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>County</th>
<th>County</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor, District 1</td>
<td>Supervisor, District 1</td>
</tr>
<tr>
<td>Alfred Hitchcock</td>
<td>Alfred Hitchcock</td>
</tr>
<tr>
<td>Vincent Price</td>
<td>Vincent Price</td>
</tr>
<tr>
<td>Write In</td>
<td>Write In</td>
</tr>
</tbody>
</table>
Proof-of-Concept Implementation

- Packaged as malicious Windows scanner driver
- Tested with Fujistu fi-7180 scanner
  - EAC certified for use in U.S. elections: Clear Ballot’s ClearVote system
Testing across ballot styles

- Four largest U.S. election vendors
  - ES&S, Hart InterCivic, Dominion, Clear Ballot

- Two older styles of ballots
  - Hart InterCivic, Diebold
Marking Ballots

- Bajcsy systemization
- Prepared 720 marked contests
  - 120 per ballot style
- For each ballot style:
  - 60 “Filled” marks
  - 10 of each marginal mark and 10 empty
Key insight!

- We only need to move marks we can confidently manipulate without leaving artifacts – ensure not visibly noticeable that marks have been moved.

- We only have to move enough marks to change result: realistically only small fraction, people need to believe result.

Example ballot we would not manipulate.
## Performance of UnclearBallot

<table>
<thead>
<tr>
<th>Ballot Style</th>
<th>Invalid Marks</th>
<th>Valid Marks</th>
<th>Time / Success</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Skipped</td>
<td>Success</td>
<td>Failure</td>
</tr>
<tr>
<td>Clear Ballot</td>
<td>55</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Diebold</td>
<td>60</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dominion</td>
<td>38</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>ES&amp;S</td>
<td>52</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Hart (eScan)</td>
<td>60</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hart (Verity)</td>
<td>60</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Feasibility in real election

- For every style of ballot, we were able to move at least 18% of ballot marks. Could swap results in 48/51 districts in 2016 election
  - Wyoming and WV are only red districts that could not have been turned blue
  - D.C. is only blue district that could not have been turned red
- Not realistic for Wyoming to vote blue, wouldn’t be believed
- Shows that in a close election we could change the results
Testing with Real Voted Ballots

- Corpus of scans of 181,541 real ballots
  - Nov 6, 2018 General Election Clackamas County, Oregon
  - Votes centrally counted with optical scanner
  - Hart Verity-style
### Measure 102

**Referred to the People by the Legislative Assembly**

Amends Constitution: Allows local bonds for financing affordable housing with nongovernmental entities. Requires voter approval, annual audits

**Result of “Yes” Vote:** “Yes” vote allows local governments to issue bonds to finance affordable housing with nongovernmental entities. Requires local voters’ approval of bonds, annual audits, public reporting.

**Result of “No” Vote:** “No” vote retains constitutional prohibition on local governments raising money for/loaning credit to nongovernmental entities; no exception for bonds to pay for affordable housing.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

### Measure 102

**Referred to the People by the Legislative Assembly**

Amends Constitution: Allows local bonds for financing affordable housing with nongovernmental entities. Requires voter approval, annual audits

**Result of “Yes” Vote:** “Yes” vote allows local governments to issue bonds to finance affordable housing with nongovernmental entities. Requires local voters’ approval of bonds, annual audits, public reporting.

**Result of “No” Vote:** “No” vote retains constitutional prohibition on local governments raising money for/loaning credit to nongovernmental entities; no exception for bonds to pay for affordable housing.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

---

**Real Ballot Results**

- **Rejected 20,117 (11%)**  
  - Scanning glitches
- **Conservative parameters**
- **Altered 62,400 (34%)**  
  - Random sample inspected  
  - No visible artifacts
- **Alteration time: 279 ms**
- **Hart scan time: 352 ms**
What good are image audits?

- Useful for catching non-adversarial error
- Identify and document discrepancies
  - 2,000 ballots discovered missing in Maryland in 2016
  - Identified flaw in ES&S DS850 high speed scanner: some ballots were sticking together
- Cannot be relied upon to detect attacks
Detection?

- Detecting image manipulation is an arms race at best
- Likely that attacker could gain access to detection code
  - Could improve manipulation algorithm
  - Could use detector as part of mark-moving algorithm
- To our knowledge, no vendor does even minimum automated detection today…
Securing against image manipulation

- Best solution is to do an RLA where people are looking at physical ballots
- Fully software independent
- High probability of detecting and correcting any outcome altering, error, or fraud even if all election equipment has been infected with malware
Conclusions

- Image audits involve checking a digital photo of the ballot
- However, an attacker could use computer vision techniques to automatically alter ballot images to show a different result
- We implemented this with an EAC certified scanner
- Attack works across widely used ballot styles from all major vendors
- Best defense: people audit physical ballots - software independence
<table>
<thead>
<tr>
<th>State</th>
<th>Governor</th>
<th>Vote for One</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amelia Earhart</td>
<td>Amelia Earhart</td>
<td>X</td>
</tr>
<tr>
<td>Howard Hughes</td>
<td>Howard Hughes</td>
<td>O</td>
</tr>
<tr>
<td>Charles Lindbergh</td>
<td>Charles Lindbergh</td>
<td>O</td>
</tr>
<tr>
<td>Write In</td>
<td>Write In</td>
<td>O</td>
</tr>
</tbody>
</table>