ACCURATE

A CENTER FOR
CORRECT, USABLE,
RELIABLE, AUDITABLE,
AND TRANSPARENT ELECTIONS

Applying a Reusable Election Threat Model at the County Level

Eric L. Lazarus
David L. Dill
Jeremy Epstein
Joseph Lorenzo Hall

Motivation

- Legitimacy of government depends on trustworthy elections.
- Potential for *undetected* fraud undermines the basis for trust.
- Elections are extremely attractive targets for fraud.
  - Attackers may be highly motivated.
  - And have access to massive resources.
- Primary responsibility for fraud prevention/detection rests on local election officials.

ACCURATE

Scope

- Focused on attempts to steal election without detection.
  - Injecting fraudulent ballots into system.
  - Changing results after ballots are cast.
- Did not consider
  - “Robbery in broad daylight”.
  - Mistakes, breakdowns, etc.
  - Deniable but detected attacks.
  - Vote suppression.
  - Misleading campaigns.
  - Sabotage of campaigns.
  - Etc.

Importance of procedures

- Even the best election technology cannot prevent fraud.
- Optimal procedures are crucial.
  - Physical security of ballots.
  - Auditing (broadly construed).
  - Public observation (to deter insider attacks).
- Achieving an acceptable level of security is *highly nontrivial.*

Systematic Threat Evaluation

- Election security is a tough, complex problem.
- How should scarce resources be allocated?
  - Need *quantitative* comparison of threats and countermeasures.
  - Which threats to address first?
  - At what price?
- Also helps with larger policy debates (e.g., electronic/internet voting).
- *But how can we do it?*

Proposed solution

- Systematic, quantitative threat modeling at the local level.
- Based on (generalized) attack trees (AttackDog tool).
- Major challenge: How to make it feasible?
- Solution: Tailor a generic, reusable threat model to the particular jurisdiction.
- We tested this idea in Marin County, CA, in the November 2010 general election.

Marin County, CA

- Medium-size county (pop. 242,409) just North of San Francisco (across Golden Gate Bridge).
- With very patient and helpful election officials (esp. Elaine Ginnold – THANKS!)
- Uses precinct-count optical scan voting + central count optical scan.
- Lazarus and Hall
  - Interviewed staff.
  - Observed on Election Day.
  - Observed post-election hand audits.

Threat evaluation methodology

- *<Figure out how to explain AttackDog concisely>*
- *Picture of attack tree, with key concepts?*
- *Goals, and/or nodes, attack steps*
- *Attacks, attributes, attack cost.*
- *Reusable parameterizable subtrees.*
- *“Omit” nodes.*
- *Defense domain.*
- *Computing attack cost*
- *COST CAN BE ANYTHING.*
- *Distinguish CAPABILITIES from APPLICATION in this case.*

Attack Team Size (ATS)

- Metric for attack team cost.
- ATS = number of people knowingly involved in the election fraud.
- Justifications
  - Major consideration: risk of detection.
    - May thwart goal.
    - May incur penalties.
  - Relatively simple (minimizes number of “judgement calls”).
  - Not misleadingly precise.

ACCURATE

Reusable threat model

- Began with very detailed general threat model.
  - Developed over several years.
  - Learned from Leon County, FL
  - Incorporated aspects of EAC model (TIRA) (Yasinsac).
- Learn jurisdiction-specific details
  - Focus on critical aspects, based on existing tree and knowledge (e.g, auditing, physical security).
  - Observe procedures in practice.
    - Polling place procedures.
    - Ballot transportation and storage.
    - Auditing procedures.
- Set parameters appropriately
- Change model (hopefully, not much).

Model adaptations for Marin

- Parameters
  - Estimated # of voters, polling places.
  - # of poll workers/polling place.
  - # of members of each ballot counting team during manual audit.
  - Qualitative parameters (stringency of tamper evidence measures and audit procedures).
  - Election assumptions: Margin of victory, # of votes that can be stolen in a precinct or machine without being obvious.

Model extension

- Ballots are transported from polling places to election office in two stages:
  - Poll workers take ballot boxes to “drop-off centers”.
  - Many boxes are loaded into trucks for transportation to final destination.
- This has an impact on ATS, because small teams have access to many ballots during the second stage of transportation.

Computer security is useless*

- There are infinitely many ways to subvert computer systems with ATS = 1.
- Securing machines is hopeless (from this perspective).
- Only hope for increasing ATS is to used audited “software independent” systems.
- (We did not evaluate computer security in Marin.)

*for increasing ATS

Malware attack

- Subvert voting technology
  - Make voting machines cheat using malware.
  - Steps: Write malware, insert malware, evade testing, etc.
  - *Must also defeat California manual auditing process of paper ballots.*
    - Tamper with paper ballots during transportation or storage.
    - Insider attacks on audit process.
      - Non-random precinct choice.
      - Defeat comparison of hand count with committed total.

Vote by mail attacks

- Obvious: Election office insiders could discard ballots (1 insider).
- Less obvious: “Stolen registration” attack
  - Small number of attackers registers many legal but never-registered voters (1 insider at Dep’t. of Moter Vehicles has this info).
  - Requests absentee ballots be sent to various addresses.
  - Small team fills out many ballots and mails them in.

Weighted attack team size

- Alternative metric: Insiders are "more costly" than outsiders on attack team.
  - Rationale: Insiders are harder to recruit, may be more carefully vetted.
  - We tried: 1 insider = 10 outsiders (easy in AttackDog).
  - Shifts low-cost attacks to outsiders
    - Subverting audited ballots – 2 outsiders.
    - Discarding VbM ballots – 10 (1 insider).
    - VbM "registration theft" – 8 outsiders.

ACCURATE

Discussion

- Threat evaluation with reusable threat models may be practical.
- Even with paper ballot systems and audit requirements, security is tough.
  - Physical security of ballots.
  - Auditing is very sensitive to procedural details.
- This study is a first step, not a solution.

Future

- Tool improvements
  - More efficient evaluation under multiple scenarios.
  - Better summarization of possible attacks.
  - General “productization”
- Make the problem simpler
  - Simplified elections.
  - Standardized security for election jurisdictions.
  - Individual ballot auditing.

Who should do evaluations

- Independent
- experts
- using standard threat models
- evaluating standard procedures