E-Voting and Forensics: Prying Open the Black Box

Sean Peisert Matt Bishop
Candice Hoke Mark Graff David Jefferson

given at
EVT/WOTE'09
Montreal, Canada
August 10, 2009

Key Questions That We Address

- What questions can a forensic examination answer?
- When should election administrators consider an election forensic examination?
- How should they prepare for an examination?
- Who should be included on the forensic team?
- What sort of legal, contractual, and practical provisions may be needed?

Key Questions We Do *Not* Answer

- Study the merits of e-voting, or specific types of e-voting systems.
- Analyze or discuss proposed voting systems.
- Analyze specific auditing techniques.

Some Causes of Problems in Voting

- Malicious attacks can occur.
- Many problems are caused by accident and are not malicious.
    - Someone trips over a power cord.
    - The polling place floods due to rainstorms.
- Basic Problem: what happens when something goes wrong with an election?

Questions Driving Election Forensics

- Why don’t vote totals always reconcile?
- Why does a system keep failing?
- Are totals accurate and complete?
- Can election officials certify the results?
- Will the public accept the results?
- Should candidates demand a recount?

Issues With Election Forensics

- No generally/broadly accepted logging/ auditing standards.
- No generally/broadly accepted machine standards.
- No concrete legal guidance from court precedents.
- In forensic auditing, accountability and traceability are key. But votes cannot be tied to individual voters.

Privacy and Security Must Be Balanced

(Peisert, Bishop, & Yasinsac HICSS'09)

- Election officials need to be able to count ballots
- Forensic analysts need to be able to determine if and how a machine failed.
- Cannot allow a voter to indicate to an auditor who they are (vote selling)
- Cannot allow an auditor to determine who a voter is (voter coercion)
- This leads to a direct conflict.

What About VVPATs?

- VVPATs are not audit trails (Yasinsac & Bishop, HICSS'08)
- If a VVPAT shows an undervote:
  - could be malfunction
  - could be voter choice
- If a VVPAT shows an over-vote:
  - probably malfunction, but where?
- If a VVPAT shows an equal balance:
  - implies that any problem did not involve dropping or adding votes (but could simply be mis-recording votes)

Questions a Forensic Examination Can Answer

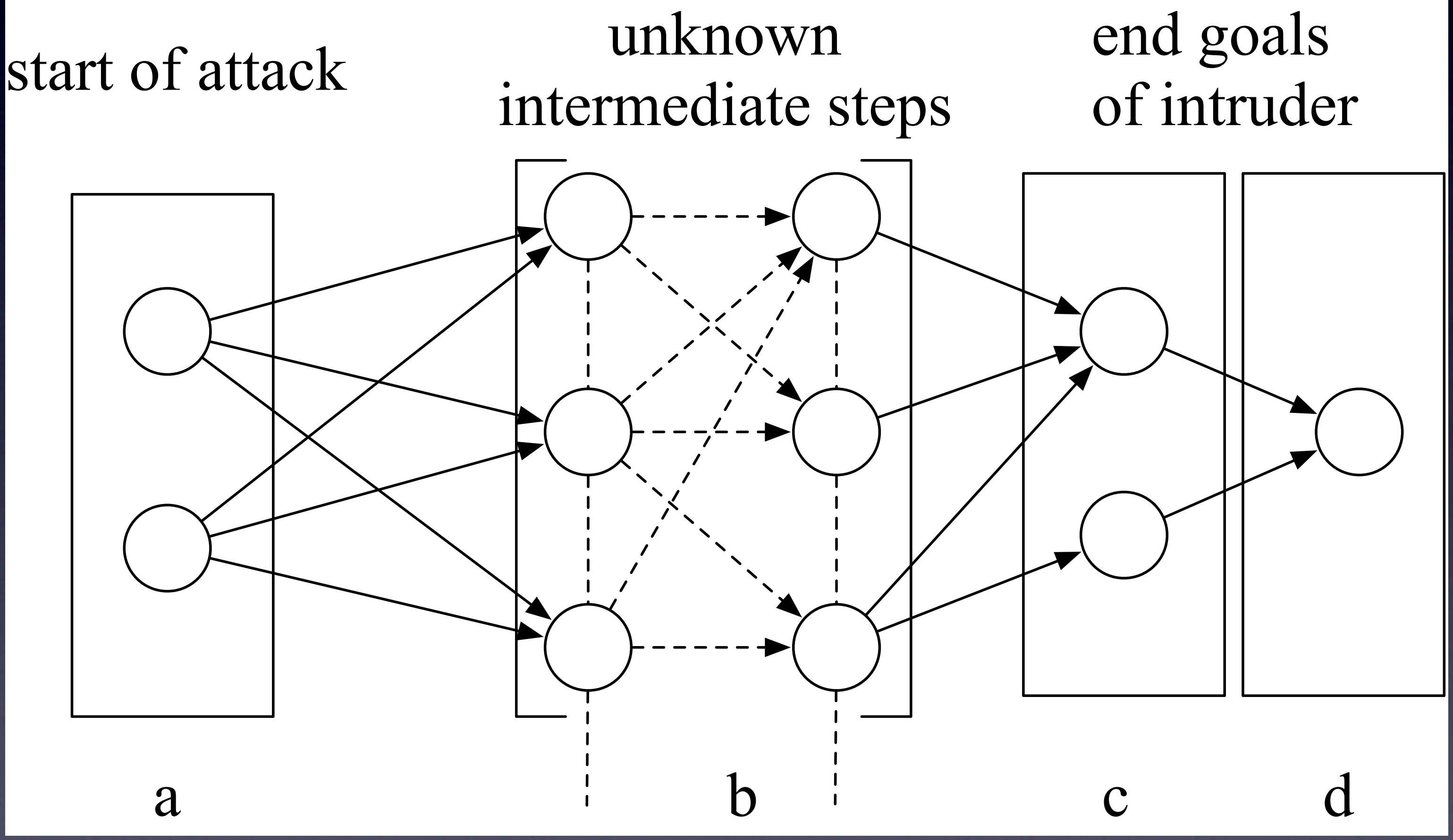
- How many votes did the problem affect?
- How accurate are the canvass totals?
- If the totals are wrong, can the investigation recover the data needed to correct the problem?
- Is the voting equipment functioning according to documentation?
- Were any procedural guidelines violated?
- Which jurisdictions does the problem affect?
- ...and others...

Requirements

- Accuracy
- Availability
- Secrecy
- Anonymity

Laocoön: A Model of Forensic Logging

- Our approach: what data do we need to record in order to be able to analyze certain events?
- Attack graphs of goals.
- Goals can be attacker goals (i.e., "targets") or defender goals (i.e., "security policies")
- Predicates represented by pre-conditions & post-conditions of events to accomplish goals.
- Method of translating those conditions into logging requirements.

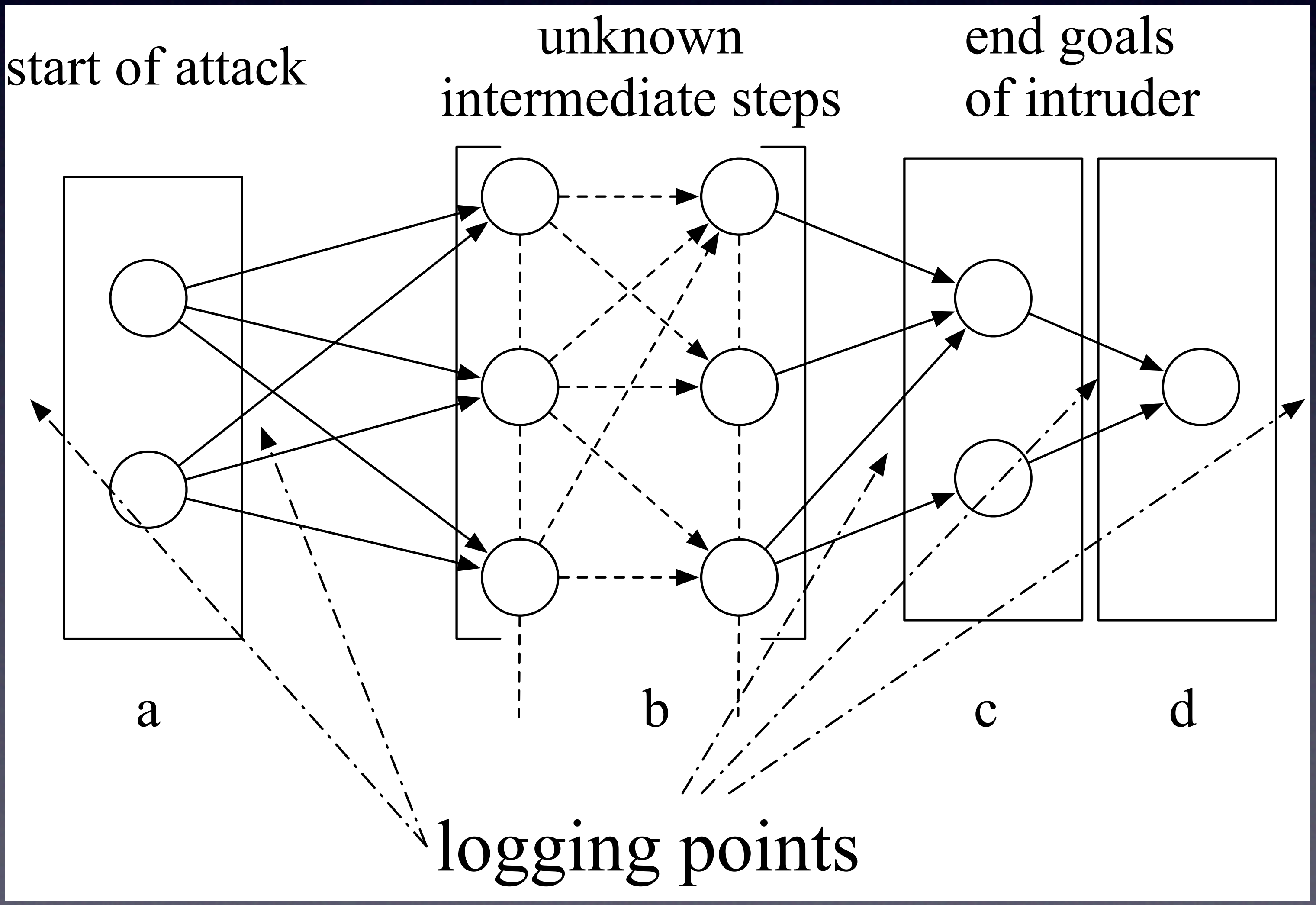


Laocoön & E-Voting

- Many violations of security policy on e-voting are easy to define precisely (e.g., changing or discarding cast votes)
- Machines have (theoretically or ideally) limited modes of operation.

Applying the Model to E-Voting: Start with E-Voting Requirements

- Laws and requirements become security policies
- Security policies define attack graphs
- Attack graphs start with ultimate "goals"
- Attack graphs are translated into detailed specifications and implementations to guide logging



Law to Policy

- California Constitution, Article 2 ("Voting, initiative and referendum, and recall")
  - Law: *Sec. 7. Voting shall be secret.*
  - Manual Voting Policy: the person who opens envelopes containing absentee ballots and removes the ballots is different than the person who tallies the ballots.
  - E-Voting Policy: information must not "leak" outside the system through any method other than the prescribed ballot.

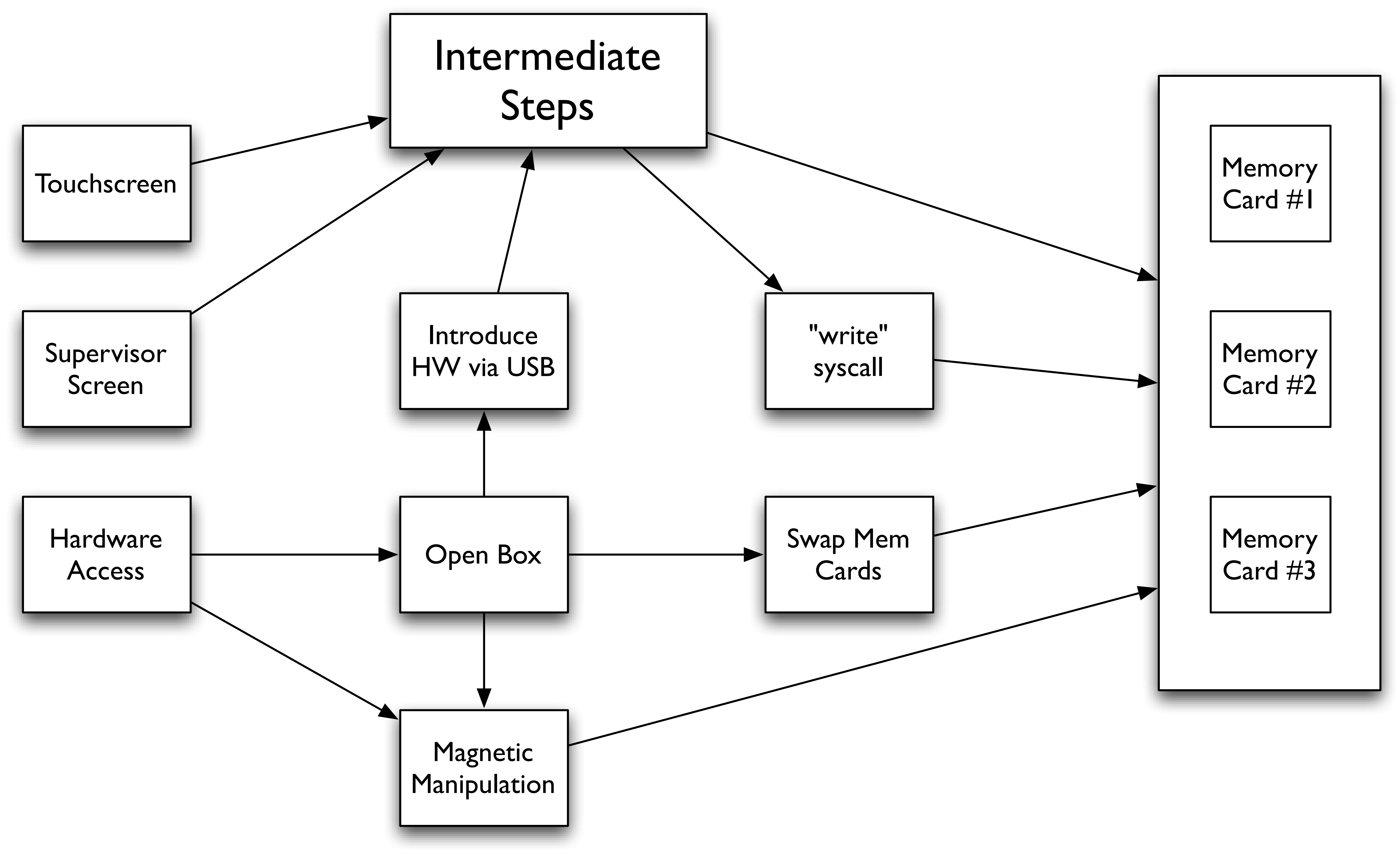
Policy to Goals

- Examine the ballots for signs of unique identifiers.
- Examine the setup of the e-voting machines to see if network cables, wireless devices, or physical sight lines could cause votes to be observed.
- Interview poll workers to determine the locations of people during voting.

Example: Laocoön & Over-Voting

- Over-voting occurs when more candidates are selected than allowed in a given race.
- At some point, the value of a bit changes.
- What are the paths to that event?
  - Start with the entry to the system (e.g., touchscreen, supervisor screen, HW manipulation).
  - End at the data.
  - This places bounds on the intermediate steps.
  - Monitor those paths.

Laocoön & Over-Voting



Procedural Elements

- What about methods of bypassing the logging system?
- How tamperproof are logs?
- What about denial-of-service?
- What about human error?
- What about DREs vs. optical scanners?

Basic Concept

- Repeated crashes, freezes, or auto-reboots may indicate a failure of the system.
- This describes a goal state of the fault graph.
- The model states that data to describe the system and failure should be recorded.

What Data to Preserve

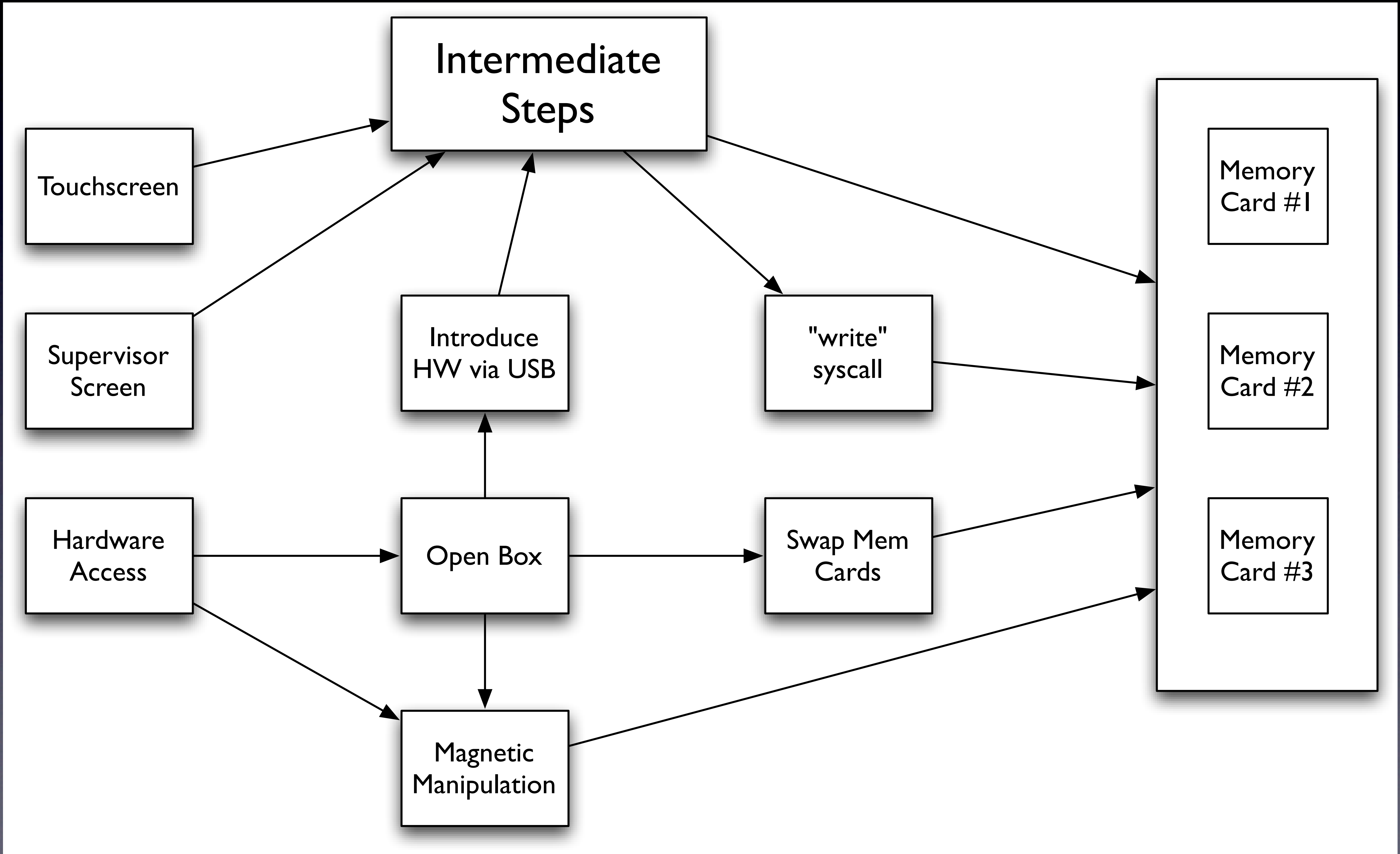
- Laocoön prescribes the need to begin with the endpoint of the attack/fault graph and work backwards to understand prior indications. Thus:

- *Rule P1: Record indications of any failure, what happened, when it happened, and any error indicators.*

Laocoön and Data Preservation

- System-level events
  - Commands capable of performing such actions
- Human events
  - Who was using the machine?
  - Who had access to the machine?

Laocoön and Data Preservation



What Data to Preserve

- Laocoön also prescribes the need to start at the beginning of the fault graph. So:
- *Rule P2: Record information about entry points into the system, including the locations from which people accessed the system.*
    - Voter interface
    - Maintenance bays
    - Include non-voters, such as officials and vendors
    - Visual descriptions of the state of entry points
    - Locations of power cords, weather, etc...

What Data to Preserve

- Laocoön prescribes the need to record possible paths from initial states to error states. So:
- *Rule P3: Collect external data relevant to the state of the voting system*
  - VVPATs
  - Audit logs
  - Memory cards
  - Removable peripherals (e.g., USB sticks)
  - Cables indicating network/telephone connections
  - Videotapes
  - People!
  - Chain of custody details

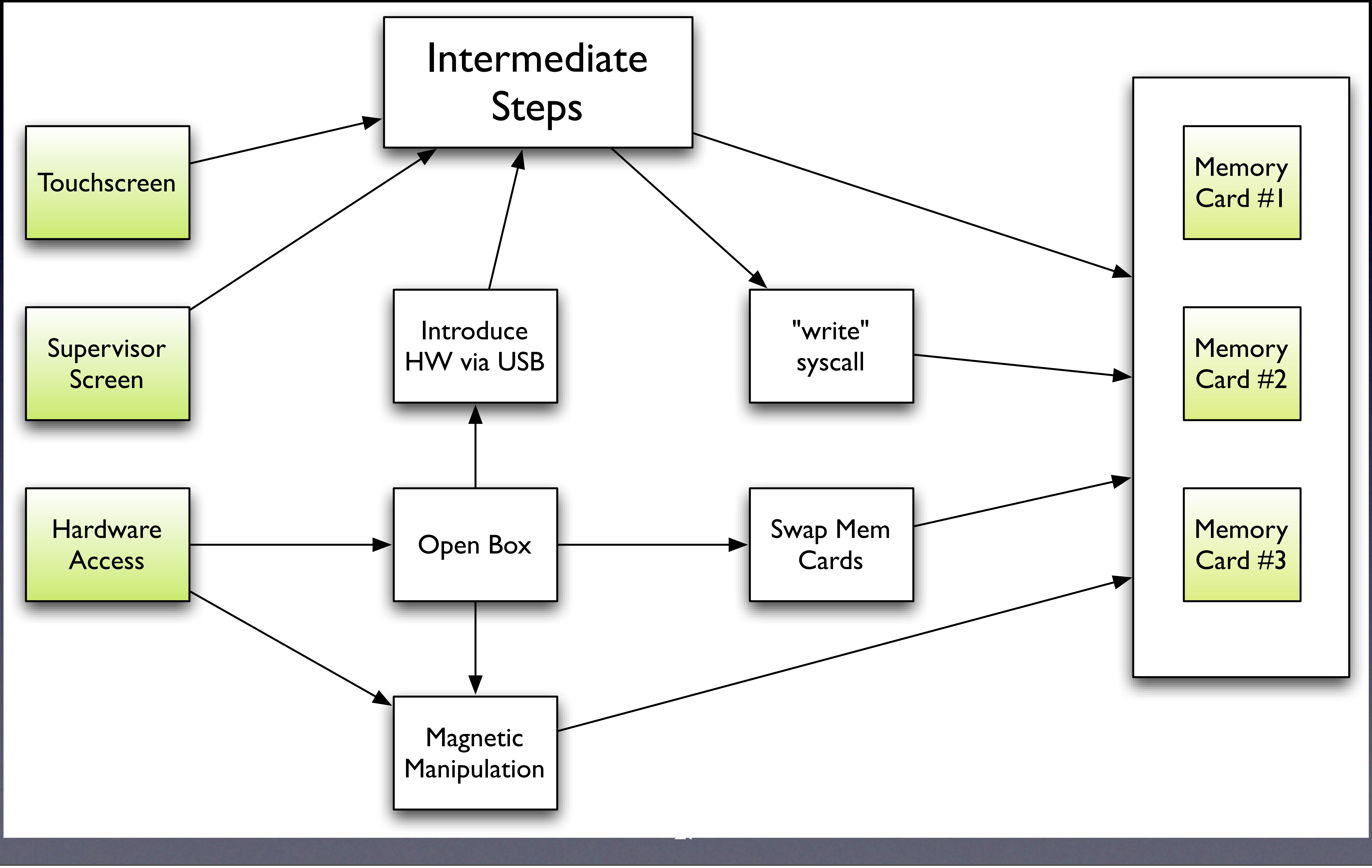
What Data to Preserve

- Laocoön prescribes the data necessary to analyze an event, and thus also the data not adhering to that standard. So:
- *Rule P4: Record any signs that the data is incomplete or may not be trustworthy*
    - E.g., if a system is supposed to record all occurrences of *X* but does so only intermittently.

Assurance and How to Preserve Data

- Laocoön prescribes that data should be recoded at failure points (both temporally and physical proximity).
- *Rule A1: Preserve all artifacts as soon as the problem is discovered, in the state in which the problem was discovered.*
    - Copies of data, clones, backups, memory
    - Precinct devices
    - Freezing evidence
    - Digital photographs
    - Network state

Laocoön and Data Preservation



Assurance and How to Preserve Data

- A human process is equally important as a Laocoön attack graph, although sometimes more difficult to implement. Nevertheless:

- *Rule A2: Election officials must have a process documenting how to handle potential evidence*
    - Chain of custody
    - Observations from humans
    - Forensic logs
    - “Two-person rule”
    - Tamper-evidence (crypto hashes, tape)

Assurance and How to Preserve Data

- *Rule A3: Potential evidence should be frozen and secured.*
    - Only forensic examiners should have access.
    - Maintain as close as possible to original state.
    - All access must be *observable.*

Assurance and How to Preserve Data

- *Rule A4: The process for preserving evidence must be public.*
- *Rule A5:The methodology and results of the forensic examination must be public.*
- Transparency is usually preferable.
- Secrecy creates doubt and inhibits assurance.
- Confidentiality of examiners' discussions is important.
- Vendors have proprietary information.
- Voters privacy must also be protected.
  - In the California TTBR, video of meetings was broadcast, but not audio.

Summary

- Forensic analysis is difficult in general
- Forensic analysis of e-voting machines is particularly challenging.
    - Tradeoffs and contradictions
    - Varying laws, technology, and human behavior
- Voting is as mission critical as designing aircraft and satellites
    - We need good design and forensic practices
    - We need high assurance in design and analysis

Going Forward

- Compare election requirements to design and implementation of voting machines
- Apply high assurance techniques to e-voting
- Analyze inherent contradictions in security, anonymity, and secrecy within elections

In the Paper

- Providing a facility for investigations
- Investigation team organization and size
- Technical qualifications of investigators
- Non-technical qualifications of investigators
- Role of the voting machine vendor

In the Paper

- Legal, Contractual and Practical Issues
- Appendices
  - Example NDA
  - Partial List of Voting Systems Studies

Thank you