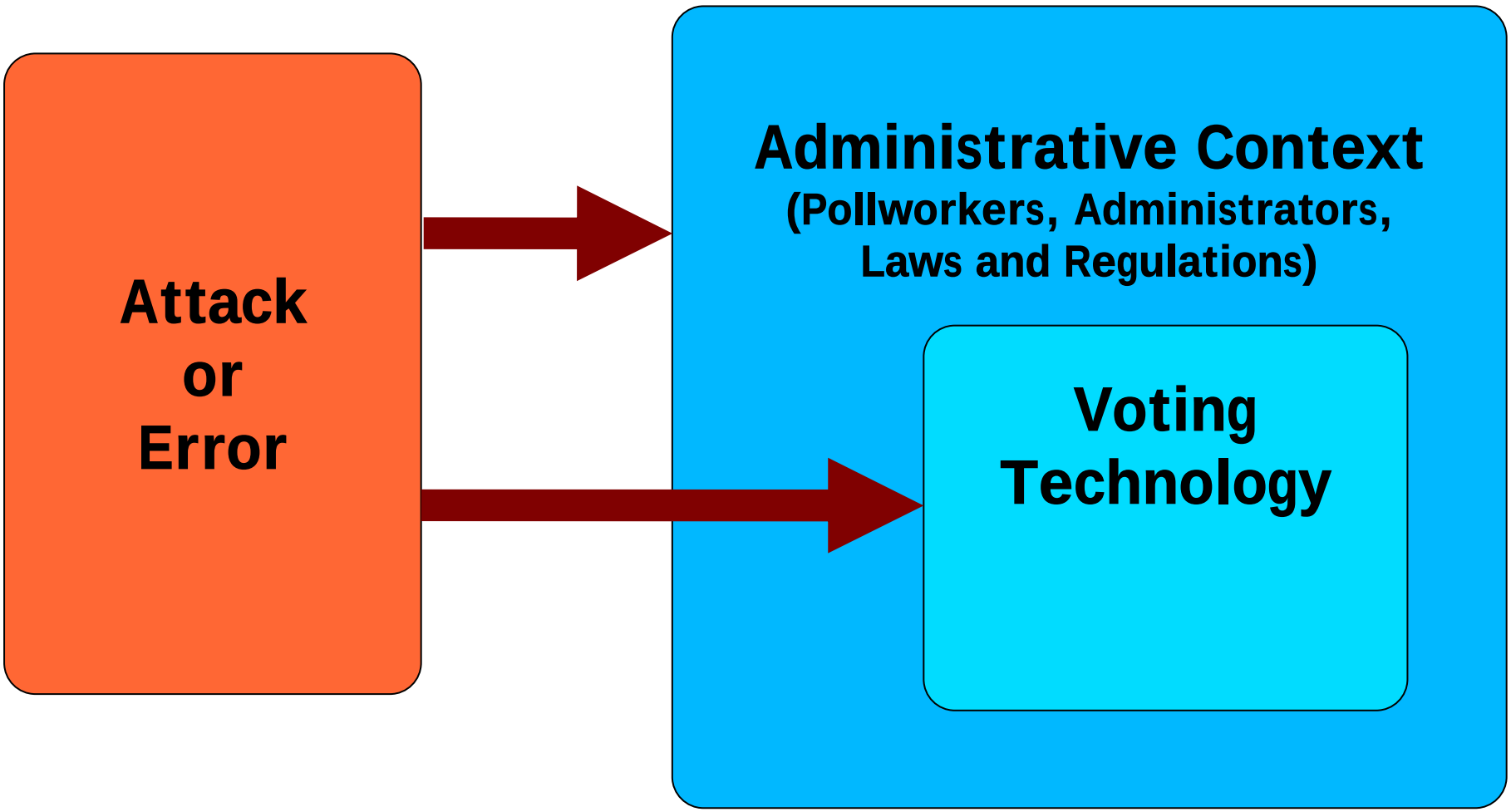
Threat Taxonomy Overview

Douglas Jones
University of Iowa

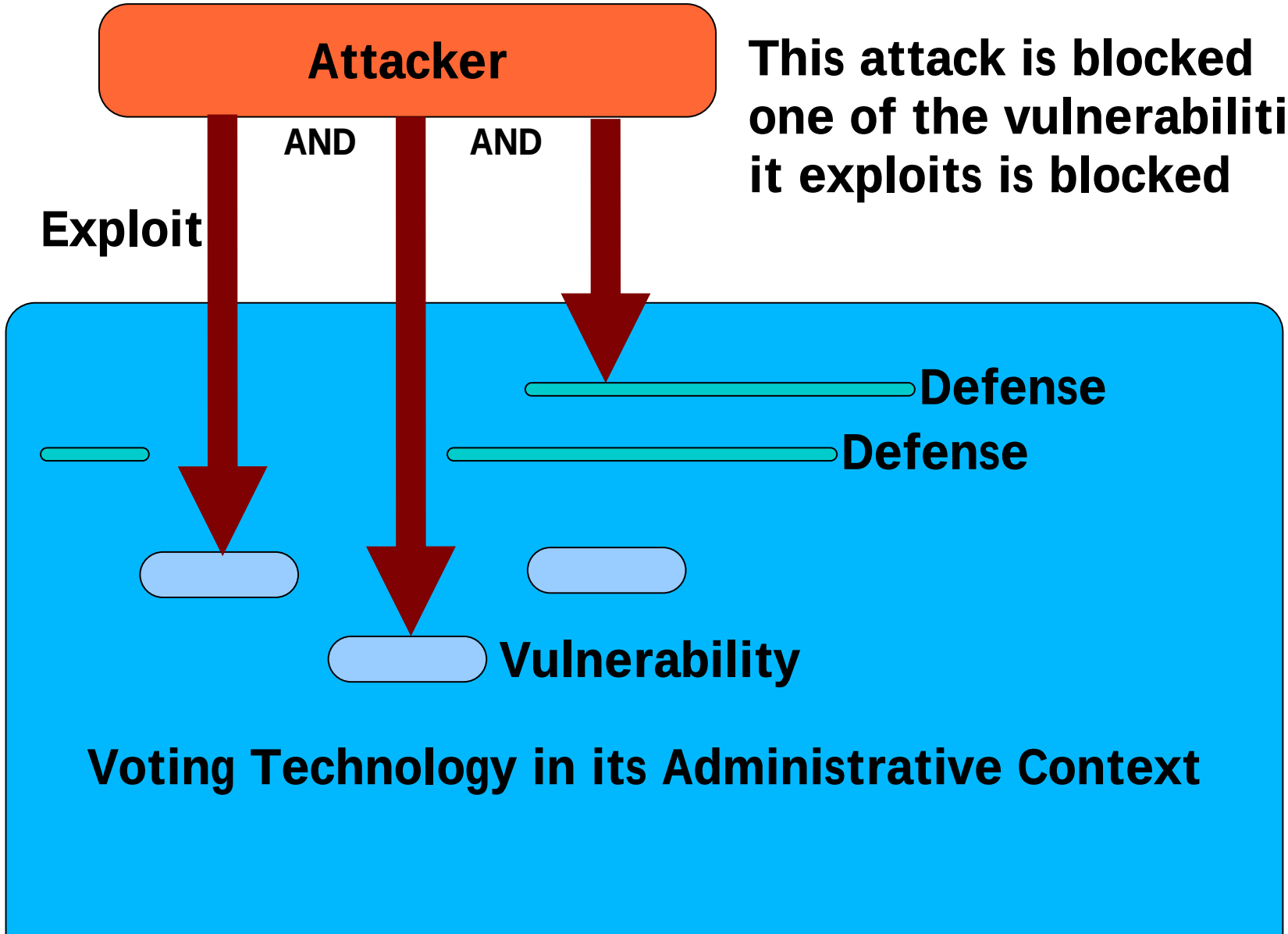
- **Voting Technology in its Administrative Context**
- **The Anatomy of an Attack**
- **A Process View of System Evaluation**
- **The Role of Threat Catalogs**
- **Taxonomy**
- **A Proposed Taxonomy**
- **If We Do This Right …**
- **A Threat Catalog is not a Threat**

the author wishes to acknowledge partial support from NSF grant CNS-052431

Voting Technology in its Administrative Context



The Anatomy of an Attack



A Process View of System Evaluation

1) Enumerate the applicable attacks

2) For each attack, identify the vulnerabilities exploited

3) For each vulnerability, identify the defenses

If all attacks are not blocked by some defense

ADD DEFENSES

This Methodology relies on knowing all possible attacks!

DEFENSE IN DEPTH:

Assume that your attacker knows something that you overlooked, so make sure that multiple defenses block each known attack.

The Role of Threat Catalogs

- The process view just outlined requires that we develop a *threat catalog*
- For each *threat*, we need to document the *vulnerabilities* it exploits
- For each *vulnerability*, we need to document the *defenses* known to block that vulnerability
- From this, we may build a *vulnerability catalog*
- From these, we can derive a *defense catalog*

Taxonomy

- Each catalogs needs organization.
- There are many dimensions to this problem:
  - What technology is vulnerable
    - paper, DRE, VVPT …
  - Who carries out the attack
    - voters, outsiders, insiders, vendors …
  - What is the scale of the attack
    - voter, precinct, county, state …
- All of these taxonomic classifications have value
- Librarians and biologists know taxonomy
  - Taxonomic systems are frequently wrong
  - A bad taxonomy may still be useful

A Threat Taxonomy

What Phase of the Voting Process is under attack

1) Registration
2) Polling place access (intimidation, violence …)
3) Voter manipulation (repeat voting, …)
4) Ballot manipulation prior to tabulation
5) Threats to the tabulation process itself
6) Threats to the result of the tabulation process

This taxonomy rests, in part, on Chapter IX of *Election Administration in the United States*, by Joseph Harris, Brookings Institution, 1934.

If We Do This Right …

We can use our threat catalog to

1) Evaluate voting systems

2) Evaluate voting system standards

3) Evaluate the administrative rules governing elections

4) Evaluate codes of election law

5) Evaluate best-practices documents

Above all, we can bring some sanity to arguments about voting technology

A Threat Catalog is not a Threat

Threat Catalogs are not a new idea

Chapter IX, *Election Administration in the United States*, by Joseph P. Harris (The Brookings Institution, 1934) was a threat catalog. He used it as suggested here.

To paraphrase Tomlinson:

Rogues know a good deal about rigging elections. "Surely it is in the interest of honest persons to know this

…

because the dishonest are tolerably certain to apply this knowledge practically, and the spread of knowledge is necessary to give fair play to those who might suffer by ignorance"