

Systemic Risk Modeling of United States In-Person Voting: Threat Analysis of Precinct Count Optical Scanners

Skylar Gayhart • Katherine Tan • Alisa Martin • Josh Dehlinger • Natalie M. Scala



Research Focus

- Precinct count optical scanners (PCOS)
- Used by ~70% of Americans voting in person during 2024
 - U.S. critical infrastructure
 - What are the risks associated with these devices? **Goals: Mitigate threats and enhance security measures**

Overview

- Extension of mail voting study (Scala et al., *Risk Analysis*, 2022)
- Current risk profile of PCOS does not exist at scale; systematically identify threats
- Calculate relative likelihood of threat
- Assess implications for risk mitigation strategies at the local level

Contributions

- Significantly updated PCOS attack tree
- First to extend threat catalog into evaluation of relative likelihood of occurrence and impact
- Practical, evidence-based toolset for targeted, local-level risk reduction
- Foundation for under-developed area in risk literature (election security at local level)



Connect with ESE

Utility of Threat

- Threat categories: Cyber, Physical, Insider
- Temporal phases: Setup, Voting, and Teardown
- Complex threat surface: Over 70,000 unique scenarios
- Delphi panel assessed relative likelihood of threats
- Utility on three dimensions related to threat:

Attack cost (AC) u_1
Technical difficulty (TD) u_2
Discovery difficulty (DD) u_3

- Relative likelihood at each terminal node X_j :

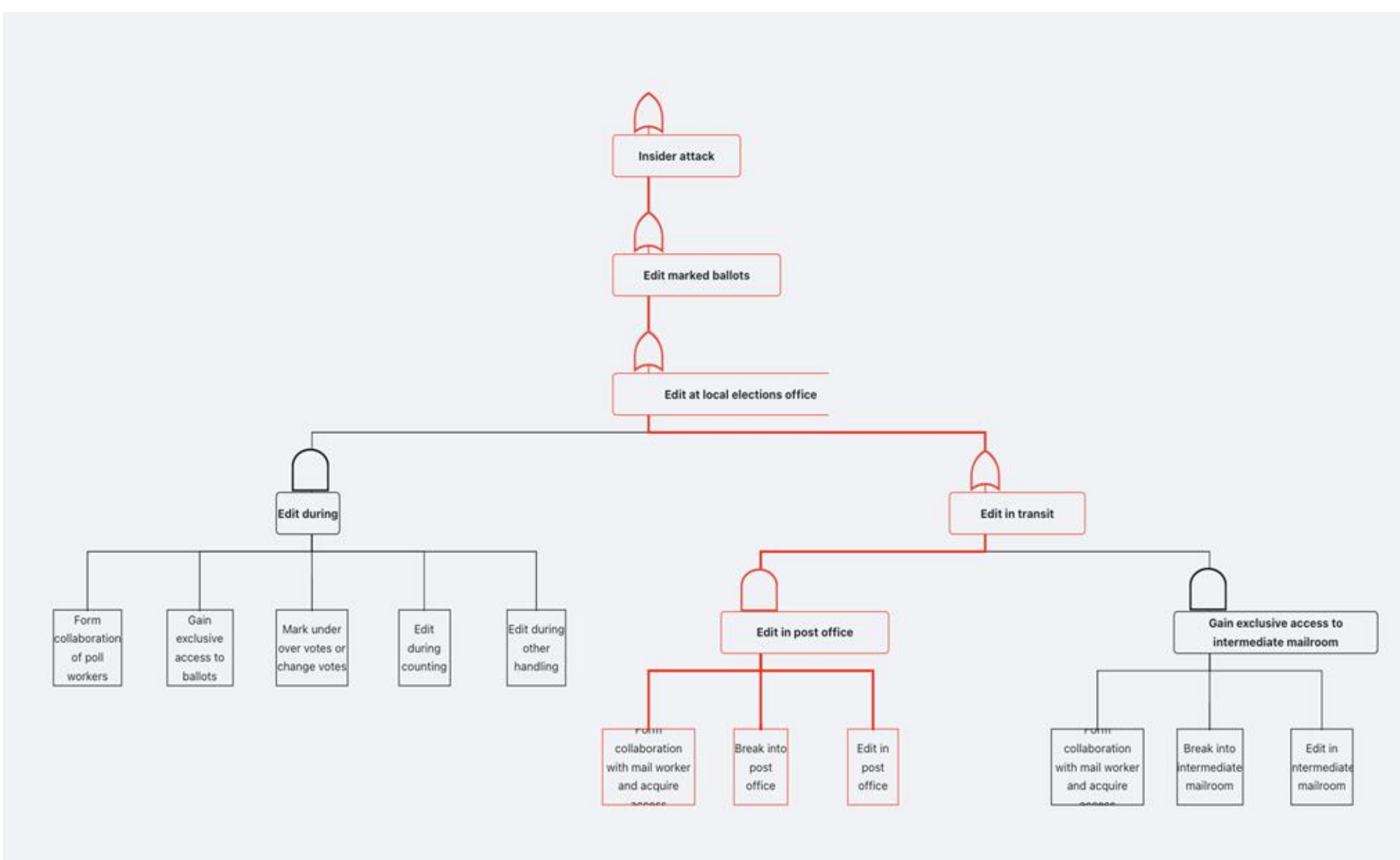
$$P(X_j) = w_1 u_{1j} + w_2 u_{2j} + w_3 u_{3j}$$

where $j \in \{1, 2, \dots, n\}$, n terminal nodes
 $w_k, k \in \{1, 2, 3\}$, weight assigned to utility function k ; $\sum w_k = 1$
 $w_k = 1/3 \forall k$

$u \in [0, 1]$, using scale factor (0.2) to convert ordinal scales

- Synthesize to system-level vulnerability:
 $S_i = (X_{i1}, X_{i2}, \dots, X_{iN})$
AND structure: $P(S_i) = P(X_{i1})P(X_{i2}) \dots P(X_{iN})$
OR structure: $P(S_i) = P(X_{i1})$
- Least likely: High cost, difficult to pursue, easy to discover
- Emphasis on comparison of scenarios, not the likelihood of any one scenario occurring

Example Scenario



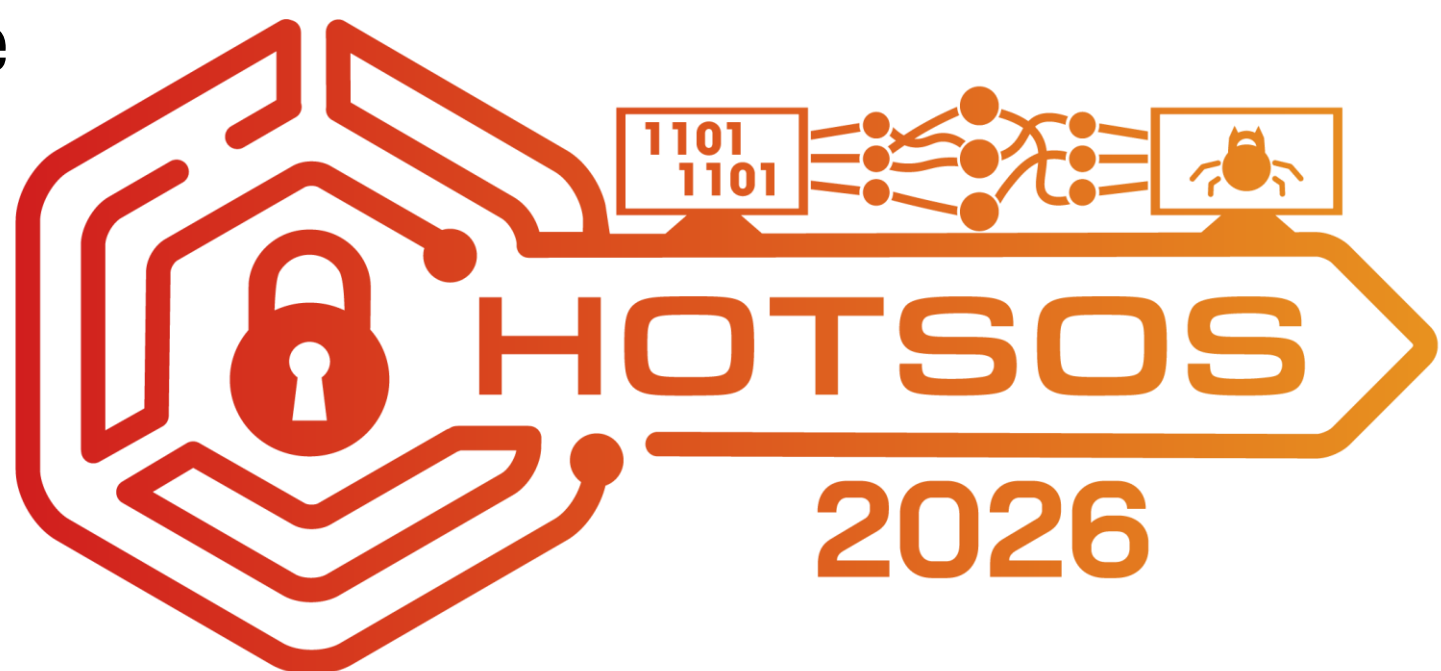
Takeaways

Threats that most impact overall system vulnerability:

- Procedural or human-factor vulnerabilities
- Interaction with voting equipment
- Device handling and logistics

60 new threats and 6 new subject areas:

- Accessibility
- Voter process error
- Misinformation voters
- Supply chain management
- Poll worker interference
- Hazardous accidents



Attack Tree Software

- Attack Tree Analysis Tool (AT-AT)
- Open-source software to visualize PCOS attack tree & outline attack scenarios
- Visualizes and evaluates relative likelihood for large scale threat trees
- Applicable to all critical infrastructure



Future Research

- Quantifying effectiveness of mitigations
- Policy recommendations to local and state election boards
- Application to other critical infrastructure sectors
- Expand framework to support decision making under resource constraints



Risk Analysis Mail Voting



Systemic Sources of Threat



Hot Topics in the Science of Security (HotSoS) Symposium
April 2026 | Hosted by the National Security Agency