Evaluating Mail-Based Security for Electoral Processes Using Attack Trees

Natalie M. Scala, Paul Goethals, Josh Dehlinger, Yeabsira Mezgebe, Betelhem Jilcha, Isabella Bloomquist

HotSoS Virtual Symposium | April 2022

Why We Are Here

TOWSON UNIVERSITY | Supply Chain Management

- Interference and attacks on U.S. voting systems
  - DHS (2017): 21 states target of attacks to voting systems during the 2016 Presidential Election
  - Senate Intel Committee (2019): Election systems in all 50 states targeted in 2016
  - Robert S. Mueller, III (2019): Interference ongoing
- DHS (2017): Election infrastructure is critical infrastructure
  - Voting systems, storage of ballots and equipment, associated infrastructure
  - Government Facilities sector

What about COVID-19?

TOWSON UNIVERSITY | Supply Chain Management

- Crowding, lines, sick poll workers were problems
- Poll workers dropped out
- Constant state of flux, plans changing, shifts in process
  - 40% of states had process change in primary
  - 47 states continued with expanded mail for General Election
- Need access in place
  - Safe, socially distant methods of voting
- Attacks on legitimacy of mail votes
- Mix of mail with in-person voting adds complexity
  - Harder for adversary to infiltrate, less impact or value

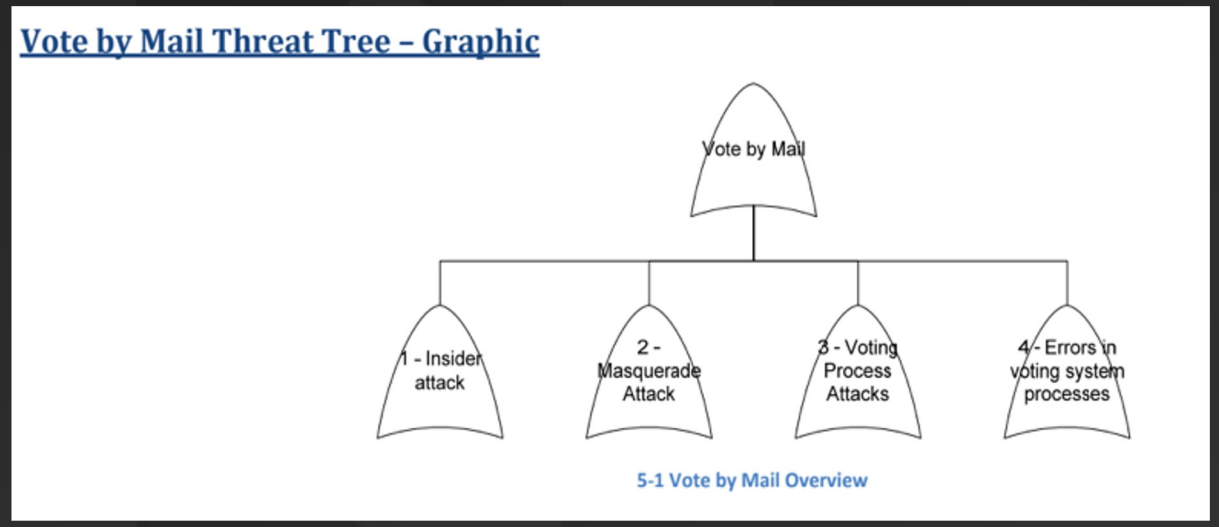
How Can Mail Voting Be Targeted?

TOWSON UNIVERSITY | Supply Chain Management

- Elections Assistance Commission (2009) attack tree data
- Attack tree is inventory of risks
  - Does not identify strength or likelihood
- Decompose complex actions into hierarchical levels
- Graphic representation of security problem
- Much has changed
  - 5 states fully or mostly mail voting
  - COVID-19
  - Adaptive adversary

Vote by Mail Attack Tree (EAC, 2009)

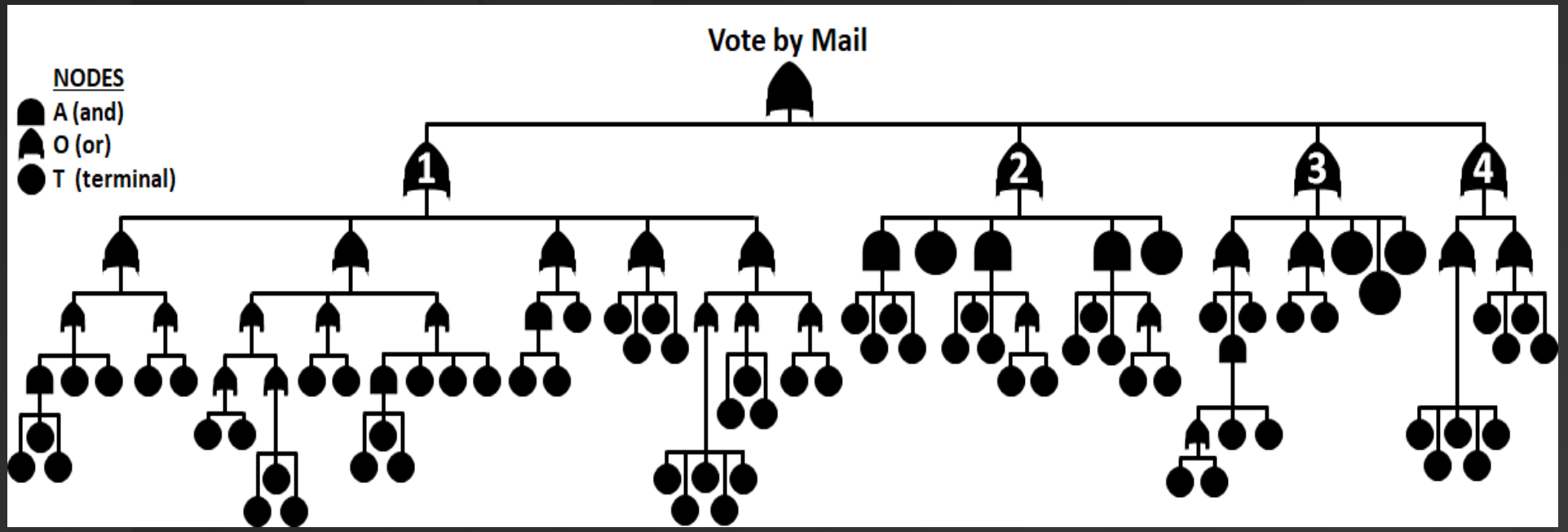
TOWSON UNIVERSITY | Supply Chain Management



node type - outline number - threat action			
O	1		Insider attack
	O	1.1	Edit Marked Ballots
		O 1.1.1	Edit at Local Elections Office
		A 1.1.1.1	Edit During Duplication
		T 1.1.1.1.1	Form Collaboration of PWs
		T 1.1.1.1.2	Gain Exclusive Access to Ballots
		T 1.1.1.1.3	Mark under/overvotes or change votes
		T 1.1.1.2	Edit During Counting
		T 1.1.1.3	Edit During Other Handling
		O 1.1.2	Edit in Transit
		T 1.1.2.1	Edit in Post Office

- Insider threats, external threats, voter error
- Hierarchy consists of *or* (O), *and* (A), *terminal* (T) nodes

Vote by Mail Attack Tree (EAC, 2009)



- Threat scenarios
  - Insider = 32
  - External = 16
  - Voter error = 9
  - Total = 57

Investigating Attack Tree Revisions

TOWSON UNIVERSITY | Supply Chain Management

Needs

- Pandemic implications
- Threats to critical infrastructure
- Adaptive adversary

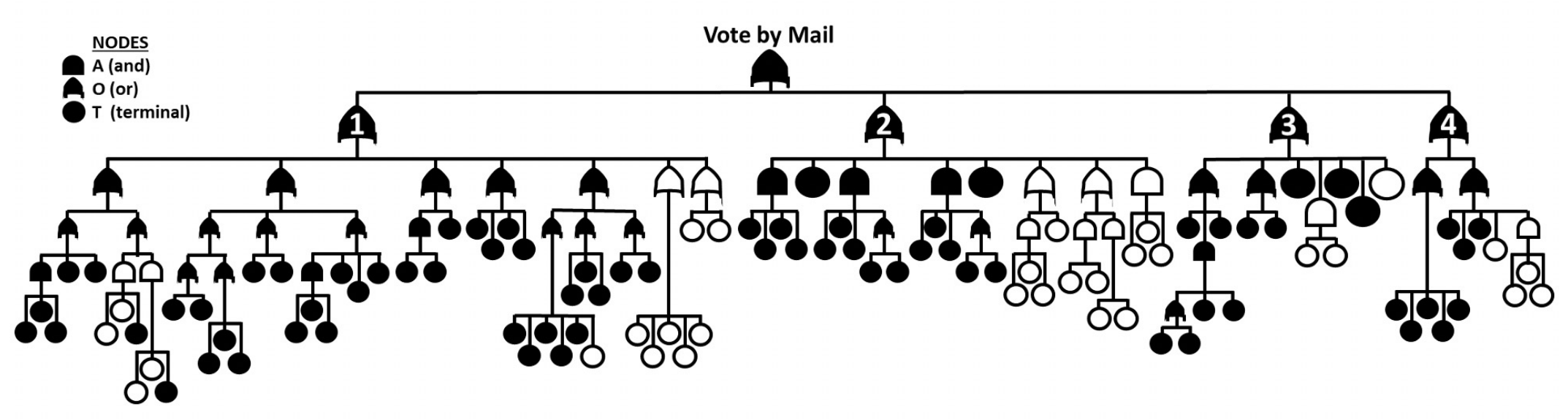
Validation

- Boards of Elections
  - Maryland counties

Sources of data

- Mainstream, non-partisan news articles
  - January through August 2020
- Bipartisan or non-political think tanks
- Academic centers
- Voter instruction sheets
- State-created documentation
- Price, et al. (2019)
- Locraft, et al. (2019)
- Scala, et al. (2020) & modules
- Poll worker training manuals

Updated Attack Tree



- 30 new threats
- Threat scenarios
  - Insider = 40
  - External = 23
  - Voter error = 10

What are the New Threats?

TOWSON UNIVERSITY | Supply Chain Management

Node	Vulnerability	Branch	Node	Vulnerability	Branch
X_{73}	Form collaboration with mail worker and acquire access	Insider	X_{88}	Destroy drop box	External
X_{74}	Break into post office	Insider	X_{89}	Gain exclusive access to ballot storage	External
X_{75}	Form collaboration with mail worker and acquire access	Insider	X_{90}	Alter marks and return to storage	External
X_{76}	Break into intermediate mail room	Insider	X_{91}	Gain exclusive access to ballot storage	External
X_{77}	Manipulate return envelope	Insider	X_{92}	Steal/destroy ballots	External
X_{78}	Misallocate polling or drop-box locations	Insider	X_{93}	Steal blank ballot from mailbox	External
X_{79}	Provide regional mail-in voting misinformation	Insider	X_{94}	Mark and return their ballot	External
X_{80}	Hinder or suppress regional postal services	Insider	X_{95}	Defeat signature check	External
X_{81}	System outage	Insider	X_{96}	Paper ballot scanner hacked	External
X_{82}	Name deliberately misspelled on ballot	Insider	X_{97}	Vote denied or altered	External
X_{83}	Paper ballot scanner hacked	Insider	X_{98}	Invalid ID card attack	External
X_{84}	Vote denied or altered	Insider	X_{99}	Error in instructions	Voter error
X_{85}	Identify target	External	X_{100}	Unclear assistance instructions when not required	Voter error
X_{86}	Acquire access to drop box	External	X_{101}	Ballot says ID required when not required	Voter error
X_{87}	Alter marks and return their ballots	External	X_{102}	Expired Voter ID	Voter error

Evaluation Measure

TOWSON UNIVERSITY | Supply Chain Management

- Strength or likelihood of threat
- Each terminal node assessed for utility on three dimensions
  - Attack cost (AC) u_1
  - Technical difficulty (TD) u_2
  - Discovering difficulty (DD) u_3
- Delphi Method
- Criteria adapted from Du and Zhu (2013)

Attack Cost (AC)		Technical Difficulty (TD)		Discovering Difficulty (DD)	
Grade	**Standard**	**Grade**	**Standard**	**Grade**	**Standard**
5	Severe consequences likely	5	Extremely difficult	1	Extremely difficult
4	High consequences likely	4	Difficult	2	Difficult
3	Moderate consequences likely	3	Moderate	3	Moderate
2	Mild consequences likely	2	Simple	4	Simple
1	Little to no consequences likely	1	Very simple	5	Very simple

Calculating Relative Likelihood

TOWSON UNIVERSITY | Supply Chain Management

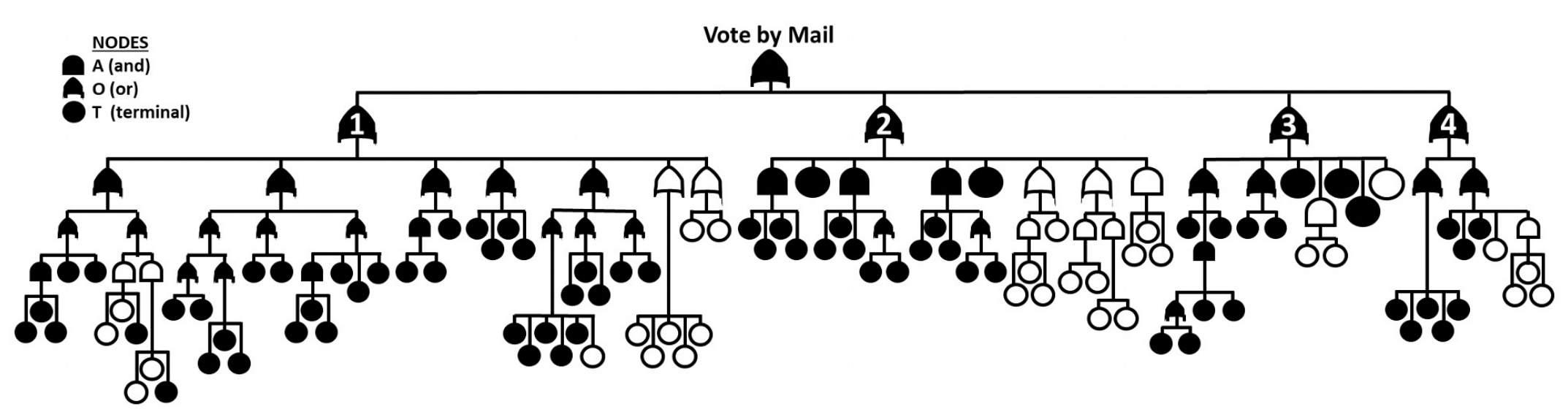
- Relative likelihood for each terminal node X_j:

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

  - $j \in \{1, 2, \ldots, n\}$, 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

Terminal Node	AC	TD	DD	Relative Likelihood	Terminal Node	AC	TD	DD	Relative Likelihood
T 1.1.1.1.1 (X_1)	4	2	2	0.08	T 2.1.3 (X_{40})	5	2	3	0.07
T 1.1.1.1.2 (X_2)	4	3	2	0.07	T 2.1.4 (X_{41})	4	2	1	0.12
T 1.1.1.1.3 (X_3)	3	4	2	0.07	T 2.2 (X_{42})	5	2	2	0.08
T 1.1.1.2 (X_4)	5	3	3	0.06	T 2.3.1 (X_{43})	4	3	3	0.06
T 1.1.1.3 (X_5)	3	4	3	0.06	T 2.3.2 (X_{44})	4	2	3	0.07

What about Scenarios?



- Threat scenarios
  - Insider = 40
  - External = 23
  - Voter error = 10
  - Total = 73

Relative Likelihood for Scenarios

TOWSON UNIVERSITY | Supply Chain Management

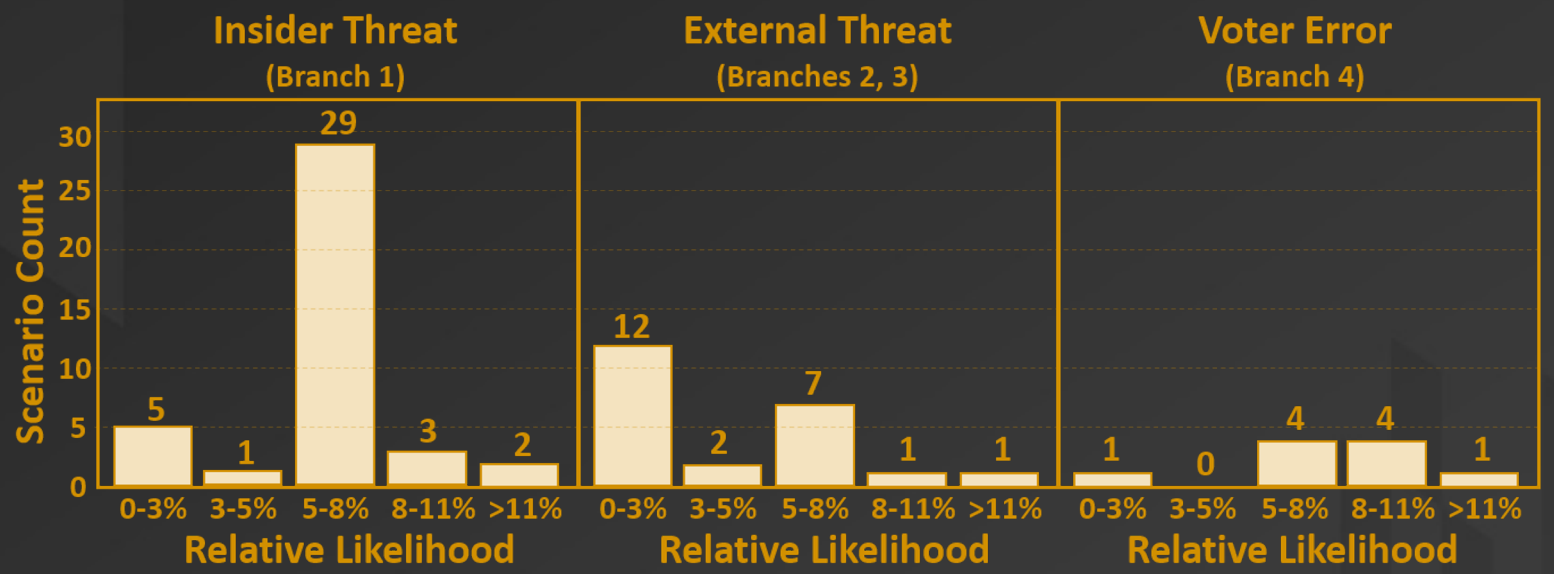
- For an attack scenario $S_i = (X_{i1}, X_{i2}, \ldots, X_{iN})$
  - AND structure: $P(S_i) = P(X_{i1})P(X_{i2}) \ldots P(X_{iN})$
  - OR structure: $P(S_i) = P(X_{i1})$
- Least likely: High cost, difficult to pursue, easy to discover

Attack Sequence	Leaf Node(s)	Relative Likelihood	Attack Sequence	Leaf Node(s)	Relative Likelihood
S_1	X_1, X_2, X_3	0.0004	S_{38}	X_{82}	0.0600
S_2	X_4	0.0600	S_{39}	X_{83}	0.0600
S_3	X_5	0.0600	S_{40}	X_{84}	0.0700
S_4	X_{73}, X_{74}, X_6	0.0002	S_{41}	X_{38}, X_{39}, X_{40}, X_{41}	0.0000

Scenario Likelihood

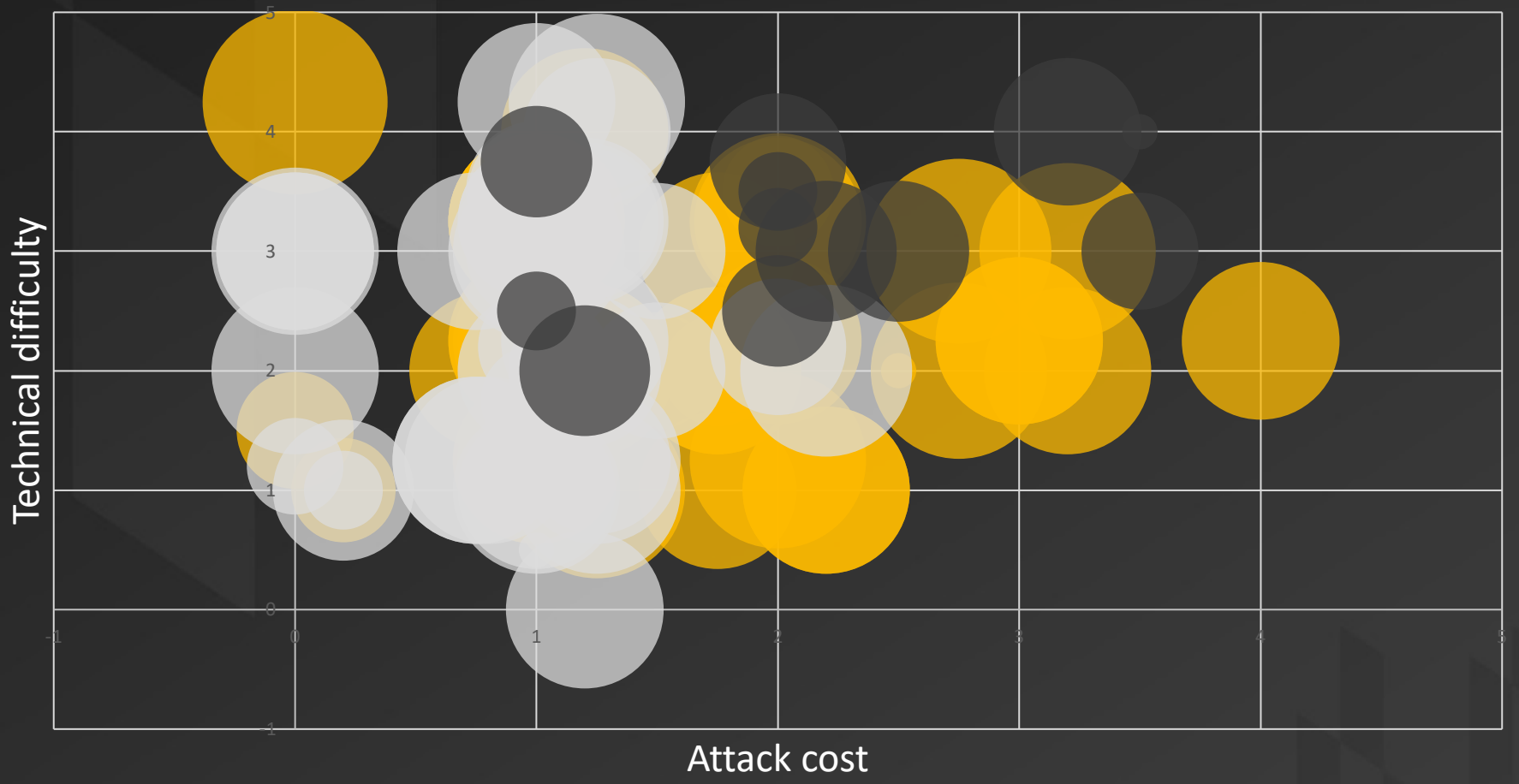
TOWSON UNIVERSITY | Supply Chain Management

- Insider: Majority of scenarios
- External: Very low relative likelihood
  - External actors may not be interested or incentivized
- Voter error: Only 13.7% of total scenarios



Threat Impact on Mail Voting

TOWSON UNIVERSITY | Supply Chain Management



- Considering attack cost, technical difficulty, discovering difficulty
- Yellow = insider threats, white = external threats, black = voter error threats

Threats of Most Concern

TOWSON UNIVERSITY | Supply Chain Management

Scenario	Threat		Relative Likelihood	Branch
S_7	X_9	Errant failed signature	0.12	Insider
S_{12}	X_{14}	Accidental loss	0.10	Insider
S_{23}	X_{28}	Fail to stuff envelope	0.11	Insider
S_{32}	**X_{36}**	**Lost in destination mailroom**	**0.13**	**Insider**
S_{47}	X_{53}	Malicious “messenger ballots”	0.10	External
S_{58}	**X_{61}**	**Debate and vote parties**	**0.12**	**External**
S_{64}	**X_{65}**	**Failure to sign correctly**	**0.13**	**Voter Error**
S_{66}	X_{67}	Failure to bundle correctly	0.11	Voter Error

- All scenarios included in EAC (2009) attack tree
- No new threats identify as high concern
- *Quick move to mail-based voting due to COVID-19 does not necessarily make the process less safe*
- Threats in bold are most likely for branch

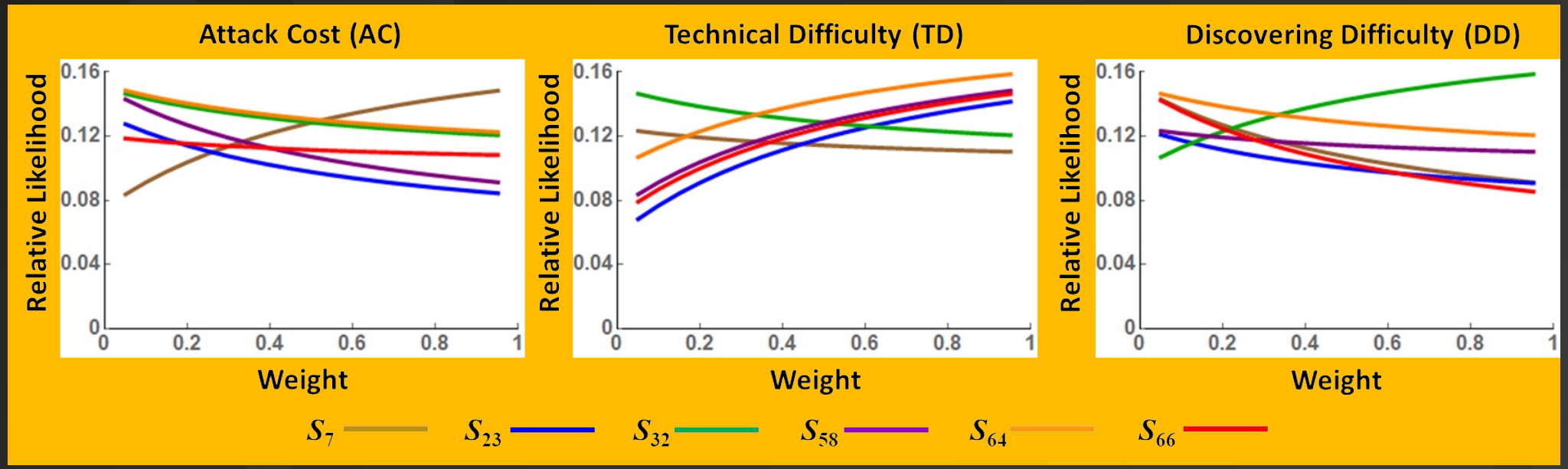
Sensitivity Analysis

TOWSON UNIVERSITY | Supply Chain Management

- All utility functions equally weighted $w_i = {}^1/_3, i = 1, 2, 3$
- What if the weights changed?
  - Evolving priorities of election officials
  - Information assurance considerations
  - Sophistication of actors
- How would relative likelihood change?
- Would that impact or change the threats of most concern?

Sensitivity Analysis

TOWSON UNIVERSITY | Supply Chain Management



- Minor sensitivity in results
- Election officials need to consider mitigations for all threats of most concern
- Most scenarios remained below 0.10 relative likelihood

Conclusions

TOWSON UNIVERSITY | Supply Chain Management

- First to consider likelihood of threat
- Updates only known attack tree for mail voting
- Majority of threat scenarios are tied to insider actions
- Extends into future as mail voting will continue to be used
  - Mail-based voting not as attractive for the adversary
  - Increases voter access
- Greater awareness of where vulnerabilities may exist and relative likelihood
  - Enable elections officials to apply security measures more effectively and efficiently

- Paper – *Risk Analysis:* onlinelibrary.wiley.com/doi/10.1111/risa.13876
- *Newsweek, AAAS, Yahoo Finance, Tucson Sentinel*
  - tinyurl.com/2p98dbbn tinyurl.com/2p9xftc4 tinyurl.com/2p83bxbd

Questions?

TOWSON UNIVERSITY | Supply Chain Management

Dr. Natalie M. Scala
Email: nscala@towson.edu
Web: www.drnataliescala.com

Dr. Paul L. Goethals
Email: paul.goethals@westpoint.edu

Dr. Josh Dehlinger
Email: jdehlinger@towson.edu

Empowering Secure Elections

- tinyurl.com/ScalaEtAl2021
- tinyurl.com/ScalaEtAl2020
- tinyurl.com/PriceEtAl2019
- tinyurl.com/LocraftEtAl2019
- drnataliescala.com/projects
- drnataliescala.com/media