Sources of Risk in Elections Security

Hannah Locraft and Priya Gajendiran
Advanced Cybersecurity Experience for Students
University of Maryland, College Park, MD 20742

Megan Price and Natalie M. Scala
College of Business and Economics
Towson University, Towson, MD 21252

Paul L. Goethals
Department of Mathematical Sciences
United States Military Academy, West Point, NY 10996

Abstract

This research examines sources of risk in voting systems, identifies potential vulnerabilities in voting processes, and establishes a risk model framework to assess and mitigate vulnerabilities. Cyber, physical, and insider threats exist in voting systems. Cyber-related threats stem from digital equipment and media, regardless if those devices are connected to the Internet. Physical threats stem from tampering with or disrupting equipment. Insider threats are related to humans interacting with the process and may involve an adversary with intent for deliberate harm or a system user making an honest mistake. This research employs a systems approach to identify potential threats to voting systems. The study examines potential patterns between system characteristics and a history of targeting through correlation analysis. The focus is on a state that uses precinct count optical scanners as a standard for a case study, identifying sources of cyber, physical, and insider threats to that equipment and process. Finally, this paper presents outlines of a preliminary risk model and generalized Markov model to mitigate and manage inherent process risk. Results of this research will enable states to understand and respond to holistic threats, and the model framework can be applied to improve processes and manage risk in voting systems.

Keywords
Elections security, correlation, influence diagram, Markov chain, risk

1. Motivation

The Help America Vote Act of 2002 transformed the way Americans vote in elections. Changes included the introduction of electronic equipment to replace paper punch cards that caused legal challenges in the 2000 Presidential election [1]. After the 2016 Presidential election, the Department of Homeland Security (DHS) disclosed that 21 states were subject to attacks on their electronic voting systems [2]. These attacks did not compromise actual votes, but continued mainstream media reporting revealed that a foreign nation state set to influence the outcome of the 2016 election [3]. Specifically, The Washington Post reported that the Russian Federation spent less than $500,000 with the goal of destabilizing our democracy and ultimately influencing the election outcome [4]. The United States is difficult to attack physically, but a cyber attack is much simpler, as systems, in this case voting systems, are decentralized, with many vulnerabilities and attack points. This decentralized nature is due to our separation of powers, with states in control of their elections. Some states have a standardized statewide process, while others do not, leaving the choice of equipment and processes up to each county’s jurisdiction. An attacker, either remotely online or physically in person, only needs to succeed in compromising one vulnerability, while the defense of systems needs to be strong and secure across all vulnerabilities. Voting system threats can be cyber, physical, and/or insider, and, due to their diverse landscape, vary between states and sometimes even within states. Thus, a systems wide approach for voting systems is needed that addresses cyber, physical, and insider components to voting systems.
This research examines sources of risk in voting systems through correlation analysis, vulnerability assessments, and risk models. Specifically, this paper examines if a state’s relative security grade is dependent on or influenced by characteristics of its voting systems and citizenry and if those system characteristics and controls potentially make the state more susceptible to attack. The research examines if the use of standardized or non-standardized policies potentially threatens overall system security and then develops a protocol for identifying threats to a state’s voting system, categorized as cyber, physical, or insider-based. As defined in Price, et al. [5], cyber threats can exist regardless of the existence of an active Internet connection in a voting system, digital machine, and/or media; physical threats involve tampering with equipment at any point in the elections process; and insider threats can stem from intentional adversarial harm or simple mistakes from honest users. This study specifically examines potential vulnerabilities at polling places, where the public interacts with the voting process and casts votes. The local level or polling place, as well as the human as an insider threat, have not been greatly addressed in the literature. Threat models focused on polling places are limited and include Lazarus, et al. [6]. This paper discusses the voting process and approach used by a county in a mid-Atlantic state and uses influence diagrams to identify classes of threats. Such analysis at the county level led to development of a preliminary risk model [5] to assess the most important potential vulnerabilities to mitigate. Finally, this paper discusses how the preliminary model extends to a Markov chain to assess risk across any type of voting equipment and when/where risk is present in the voting system. An agenda for research and a plan for the structure of the Markov model is provided. A discussion of correlation analysis is presented first.

2. Correlation Analysis

2.1 Methodology
The correlation study explored the existence of influence between the grade that a state received in a recent Center for American Progress (CAP) report [7] on elections security (i.e., their evaluation) and (i) whether the state is standardized (i.e., all counties in the state use the same voting process) or non-standardized, or (ii) whether the state uses an electronic or non-electronic pollbook. The standardization data was found through the Verified Voting website [8], and the pollbook data has been supplied by the National Conference of State Legislatures (NCSL) [9]. The study also explored if any correlation exists between the grade a state receives and the voting history of the state’s citizenry. Finally, the study also explored potential correlation between whether a state was identified as targeted in the 2016 election by the DHS [10] and each of the aforementioned attributes (standardized/non-standardized, type of pollbook, and voting history) as well as the type(s) of equipment used throughout each state. The goal of the study is to determine if the relative or perceived security of a state’s voting system may be influenced by various factors and/or if certain characteristics of a state’s system make it potentially susceptible to attack.

In order to create a correlation matrix between the election security grade received, standardization, type of pollbook, voting history, targeted status, and type of equipment used, the data for each state and the District of Columbia was coded using numerical values. Specifically, the grades in the CAP report were assigned a scale similar to a grade point average where “A” was assigned 4, “B” was assigned 3, “C” was assigned 2, “D” was assigned 1, and “F” was assigned 0. Some states were given grades such as “D/F,” so an average of the two was assigned to give a numerical value. (e.g. In the case of “D/F,” the numerical value would be 0.5.)

Standardization of voting equipment, type of pollbook, voting history, and targeted status each have binary outcomes and so are assigned values of 1 or 0. A value of 1 for standardization denotes that the state uses the same process across all counties, while 0 denotes that the state does not. Regarding pollbooks, a value of 1 is assigned if the state uses e-pollbooks; otherwise the value is 0. How the state voted in the 2016 Presidential election is used for voting history, where 1 signifies a red (Republican majority) state and 0 signifies a blue (Democrat majority) state. Finally, for targeted states, 1 is assigned if the state is identified by the DHS as being targeted in the 2016 election [10]; otherwise, it is assigned a value of 0.

The type of equipment used is represented by a weighted average of equipment used throughout the state, given by the Verified Voting website [8]. The different types of equipment (or combinations of types) listed on the website are given values from 2 to 8 based on the relative security of the equipment, where 2 represents the lowest level of security and 8 represents the highest. The security values of the voting equipment were determined using the information from the CAP report [7] and voting equipment information supplied by the NSCL [11]. The direct-
Locraft, Gajendiran, Price, Scala, and Goethals

recording electronic (DRE) voting machine without voter verifiable paper audit trail (VVPAT) is deemed to be the least secure of the four types of voting equipment and thus is assigned a value of 2. The DRE with VVPAT is assigned a value of 4, and the hand count method is assigned a value of 6. The optical scanner, which is deemed to be the most secure type of voting equipment, is given a value of 8. These values are assigned in this manner so that if a county uses multiple types of equipment, then an average of the values assigned to each equipment type can be taken and applied as a whole number. The number of counties that use each type of equipment within each state is tallied. Then, to calculate the weighted average, the percent of each state that uses each type of equipment is multiplied by the respective equipment security value (2 through 8). Finally, the products are summed for each state to find the final value for type of voting equipment. The final coded data for each state and the District of Columbia are available online [12].

2.2 Results

Table 1 presents the correlation matrix. The strongest correlation coefficient is between the type of equipment used and grade received by the Center for American Progress (0.5605). The lowest correlation coefficient is between the type of pollbook and the voting equipment a state used (0.0320).

Table 1: Correlation Matrix

<table>
<thead>
<tr>
<th></th>
<th>Grade</th>
<th>Standardized</th>
<th>Pollbook</th>
<th>Presidential</th>
<th>Targeted</th>
<th>Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade</td>
<td>1</td>
<td>0.4369</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standardized</td>
<td>0.4369</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pollbook</td>
<td>-0.1654</td>
<td>0.1195</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presidential</td>
<td>-0.4093</td>
<td>-0.0937</td>
<td>0.3919</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Targeted</td>
<td>0.1901</td>
<td>0.2071</td>
<td>0.1690</td>
<td>-0.0757</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Equipment</td>
<td>0.5605</td>
<td>0.4368</td>
<td>0.0320</td>
<td>-0.2149</td>
<td>0.2062</td>
<td>1</td>
</tr>
</tbody>
</table>

The left side of Table 2 takes a closer look at the standardization of voting processes. About one-third (37.143%) of non-standardized states use some form of DRE machines; those states tended to vote red in the 2016 Presidential election. The right side of Table 2 examines the relationship between a state’s targeted status, its standardization, and voting history. A majority of standardized states were reported as targeted (56.25%), while a majority of non-standardized states were reported as not targeted (65.71%). This makes intuitive sense; it may be easier for an adversary to attack the same process statewide instead of multiple systems and points of entry.

Table 2: Relationships Between Standardization of Voting Equipment, Targeting, and Voting History

<table>
<thead>
<tr>
<th># states + D.C.</th>
<th>Standardized</th>
<th>Non-Standardized</th>
<th># standardized states + D.C.</th>
<th>Targeted</th>
<th>Not Targeted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of states + D.C. as %</td>
<td>31.37%</td>
<td>68.63%</td>
<td>Number of non-standardized states + D.C.</td>
<td>12</td>
<td>23</td>
</tr>
<tr>
<td>% using DRE machines</td>
<td>6.25%</td>
<td>37.14%</td>
<td>% non-standardized equipment</td>
<td>56.25%</td>
<td>43.75%</td>
</tr>
<tr>
<td>% not using DRE machines</td>
<td>93.75%</td>
<td>62.86%</td>
<td>% non-standardized equipment</td>
<td>34.29%</td>
<td>65.71%</td>
</tr>
<tr>
<td>% voting red in 2016</td>
<td>50.00%</td>
<td>60.00%</td>
<td>% voting red in 2016</td>
<td>52.38%</td>
<td>60.00%</td>
</tr>
<tr>
<td>% voting blue in 2016</td>
<td>50.00%</td>
<td>40.00%</td>
<td>% voting blue in 2016</td>
<td>47.62%</td>
<td>40.00%</td>
</tr>
</tbody>
</table>

Figures 1 and 2 visualize security grades via boxplots for standardized (average = 2.375) and non-standardized (average = 1.586) states as well as targeted (average = 1.9737) and non-targeted (average = 1.6964) states. Note that standardized states have a higher security grade than non-standardized states. Targeted states also have a higher security grade than non-targeted states.

2.3 Analysis

Most of the correlation coefficients noted in Table 1 are rather weak. However, the election security grade a state receives and the type of equipment that a state uses has a moderate positive correlation (0.5605), which is the highest correlation observed in the study. A closer analysis of the CAP report [7] identifies that the type of voting machines used by states has a large impact on the grade received, which seems intuitive with our calculations. Specifically, if a state uses DRE machines without VVPAT, the state’s score is severely penalized.
The correlation matrix also has four weak correlations: standardization and grade received (0.4369), type of equipment and standardization (0.4368), voting history and grade received (-0.4093), and voting history and type of pollbook (0.3919). All other variables depicted little to no correlation.

The observed correlation among variables prompted a second analysis of the data using box plots. Standardized states tended to receive higher election security grades than non-standardized states, according to both average grades received and quartile analysis. Further analysis of the types of machines that standardized and non-standardized states use found that 6.250% of standardized states use a type of DRE machine, which equates to only one standardized state: South Carolina. However, a larger percentage (37.143%) of non-standardized states use DRE machines. This aligns with the previous finding that the CAP report penalizes states that use DRE machines, which would explain why standardized states have a higher average grade than non-standardized states. DRE machines are not considered as secure as other forms of voting equipment, as some DRE machines do not include an auditable paper trail.

The box plot of grades received among targeted and non-targeted states shows that targeted states tended to have higher election security grades than non-targeted states. This result may first appear counterintuitive but suggests that other factors may be of interest to an adversary.

3. Influence Diagrams and Preliminary Risk Model
Various types of electronic voting equipment are used across the country, and some states use multiple types of equipment across their counties. To better understand threat at the county level, at polling places where votes are cast, the study examines a mid-size county in a mid-Atlantic state as a case study. This state uses precinct count optical scan (PCOS) equipment as a standard across all counties and the process in place on Election Day is standardized as well. Interviews with Board of Elections personnel, a tour and simulation of a mock polling place, and a study of the Election Judge manual, along with an extensive academic literature review, led to an identification of sources of threat as well as potential threat scenarios. Figure 3 presents influence diagrams of sources of cyber, physical, and insider threat based upon the study and interviews. Within each influence domain, various threat scenarios are identified that could be executed in real-time at the polling place. For example, a cyber threat scenario could be hacking of the state Board of Elections database, resulting in the dissemination of malware to counties through local certified network servers. A physical threat scenario may be interception or stealing of ballots or memory cards, or replacing documents with replicas that include corrupted information. An insider threat
scenario example is a malicious actor posing as an Election Judge, then changing settings or information to corrupt the process while setting up election equipment.

The analysis of PCOS equipment led to the identification of 25 threat scenarios, including the three listed above. While there is no evidence to suggest the system has been compromised via these threat scenarios, each situation presents a potential and viable vulnerability to the Election Day process. A full discussion of the literature reviewed with a list of the 25 threat scenarios identified for PCOS and the county case study can be found in Price, et al. [5].

The 25 threat scenarios were then assessed via a preliminary risk model. Each scenario was scored based on the number of times it appeared or was related to nodes in attack tree data [13]; this data is a comprehensive list of potential ways an elections system may be attacked. The attack trees are multi-echelon, with “terminal” (T), “and” (A), and “or” (O) nodes. A value of one is given each time a threat appears in an attack tree as a T or A node, because each node represents one potential avenue of attack. If a threat is associated with an O node, then a score of a fraction of one is given. The denominator of that fraction is the count of O nodes at that echelon. All of the O nodes for each threat should add up to one, as altogether, they constitute one avenue of attack. Since O nodes rely on something else to occur first, they are generally deemed less risky and should receive a score of less than one.

Cyber, physical, and insider threat scenarios with the highest summed scores across the attack tree nodes are identified as most risky and therefore should be addressed. Clearly, this is a first attempt at identifying the most risky vulnerabilities. However, the county case study needed direction and recommendations for security improvements for the 2018 Midterm elections. The preliminary risk model provided input as to where to quickly focus limited resources. See Price, et al. [5] for a discussion of the threat scenarios that scored the highest in the preliminary risk model.

4. Markov Risk Model

The preliminary risk model is extended into a complete time series threat-based model using Markov chains. Each cyber, physical, and insider scenario is classified as either an "inside" or "external" threat. An example of an inside threat is memory storage devices not being encrypted properly. An example of an external threat is hacking of electronic poll books. Then, the voting process over time is examined. The attack scenarios, with their associated probabilities, are examined in the sequence of their potential occurrence over the entire electoral process. Using Markov chains (state of the threat at time t), one is then able to identify if, at any one time, the threat is more likely inside than outside/external. For instance, when the DRE machines are not connected to Wi-Fi or updates to the electronic systems are not being applied, the primary threat may be from an inside source. However, perhaps during the execution of the voting process (when all systems are online and connected), the threat may be primarily from an external attack. Ultimately, a time series-based Markov model that demonstrates an evolving posture can be developed and be used to assess risk over time.

The attack tree data [13] is used to identify potential threats that are further assessed via the Markov chain model. Although the preliminary risk model examines PCOS voting systems, the data [13] also includes attack trees for other types of electronic voting systems. Therefore, the Markov model framework can be applied to any electronic voting system or equipment in order to assess vulnerabilities over time and develop both mitigations and responses to evolving threat postures. Attack tree vulnerabilities with the highest calculated occurrence probabilities are
anticipated to be the simplest to carry out and the most difficult to discover. Attacks with the lowest occurrence probabilities will be of high technical difficulty and low to moderate discovering difficulty.

Future research involves completing the Markov chain based on occurrence probabilities. Such an analysis will help to identify the likelihood of a certain type of attack (cyber, physical, or insider) and when that attack is most likely to occur in the election process (set-up polling place, during voting, or tear down after Election Day). The model will also use varying probabilities of each threat to predict the likelihood of certain attack scenarios at different points in an election. Using this model will then help to identify high-risk threats to voting processes for a variety of types of electronic equipment.

5. Conclusion
The public interacts with the voting process at precincts and needs assurance that the votes cast are counted fairly and with integrity. This research identifies potential threats, examines threat patterns, and develops risk models to manage threats within voting processes. States can use the results of this research to make informed decisions regarding the type of equipment to use and the inherent risk that comes with that equipment and process design. Our goal is to enable Board of Elections personnel, who may not have technical backgrounds, to understand and manage risk, which will directly lead to improved voting process security on Election Day.

Acknowledgements
The views expressed in this paper are those of the authors, and do not represent the official policy or position of the United States Military Academy, the United States Army, or the United States Department of Defense.

References