Insider Threats to Voting Systems

Alec Yasinsac
University of South Alabama
School of Computer and Information Sciences
251.460.6290
yasinsac@gmail.com

ABSTRACT

Insider attacks are particularly insidious threats to electoral integrity. Traitors that misuse the trust that is placed in them often have system access that facilitates malicious acts themselves and their subsequent cover-up efforts.

In this paper, we define what it means to be an insider and we identify several classes of elections insiders. We also categorize the threats that each insider class has relative to the electoral functions.

Beyond specifying well-known elections insiders such as poll workers and local elections officials, we address several insider categories that are rarely, or never, mentioned in considering election insider threats. For example, we have not previously seen members of the judiciary identified as prospective elections insiders and we give a concrete example of how judges can accomplish insider attacks on elections. Similarly, we identify the impact that policy makers can have on the electoral process and show how malicious legislators may be able to influence a broad spectrum of elections through the laws that they propose and promote.

Insider attacks are real and imminent threats to electoral integrity. By identifying insiders and categorizing the threats that they pose allows us to create policies and procedures that better ensure sound elections and to ensure the integrity of our way of government at local, state, and federal levels.

Keywords

Keywords: Election Threats, Voting System Security, Risk Assessment, Secure Software

1. INTRODUCTION

Elections officials are the canonical "insider" in the electoral process. They are traditionally charged with creating election policy and procedure and with executing elections based on the policies and procedures that they created. Those are the perfect combination of authority that can facilitate undetected electoral tampering. Fortunately, these dedicated public servants have an amazing track record of accuracy and integrity under difficult conditions. Moreover, effective checks and balances have emerged that provide the voting public deserved confidence in their elections officials.

In this paper, we detail the acts and actors that constitute insider attacks on voting systems. For example, one side-effect of expanded use of technology in the electoral process is the change in the nature of the relationship between elections officials and the contracted service organizations that they employ. Elected elections officials, supplemented by temporary elections employees and citizen volunteers, have traditionally carried out critical electoral functions themselves. Outsourcing was restricted to routine tasks such as printing services, material transportation, communication, and other routine necessities where independent consultants or firms had little chance of negatively impacting any contest result. Today's increased reliance on technology has precipitated a shift of critical electoral functions, and the insider status that they endow, from elections officials to outside contractors that leverage complex technology provide specialized electoral functions.

1.1. Defining "Insider", "Attack", and "Insider Attack"

In order to rigorously examine insider threats to voting systems, we must first rigorously define the terms *attack* and *insider*. We follow up by defining their composition.

First, we define an *attack* to be an action that is intended to violate the voting system's security policy. In practice, many security policies are not formally stated, but are (often vaguely) captured in the voting process. For example, an [unstated] security policy to not reveal any preliminary results prior to the end of the voting period may be captured as a mechanism to prevent any accumulation from being conducted before the closing date and time of the voting period. Whether the policy is stated or not, an intruder attempting to accumulate and report the results prior to the close of the voting period is an attack.

The fundamental property of an *attack* is that it is an intentional violation of security policy.

For our purposes, a *voting system insider* is any person or process (hereinafter entity) in whom intentional trust has been granted. That is, an insider is an entity whose voting system-relevant behavior may reasonably be expected to be other than the most malicious possible and in whom the specific trust is codified in assignment of a designated voting system privilege, usually an access privilege to data or a process.

Finally, an insider attack necessarily involves misuse of the granted privilege by the insider in order to violate a security policy. That is, the trusted entity becomes a traitor.

Consider two quick examples to amplify these definitions. Local Elections Officials (LEOs) clearly fit our insider definition, as they are trusted officials that have privileges to access many voting system aspects. As long as they use their privileges for precisely the purpose for which they were granted[1], they will not commit an insider attack. On the other hand, it is easy to see that

GTIP 2010 Dec. 7, 2010, Austin, Texas USA Copyright 2010 ACM 978-1-4503-0446-7/10/12 ...$10.00

[1] Assuming that the security policies are valid.

an elections official that misused their trust is a voting system insider.

On the other hand, the insider status of voters is somewhat less clear, but may be more illuminating than for LEOs. Upon presentation of proper credentials, voters are granted access to the voting system in order to cast their ballot. Moreover, they are expected to use the system only for its intended purpose, that is to make their selections and cast their ballot in an election. If a voter uses that privilege, i.e. physical access to the voting system, in order to maliciously tamper with the voting machine in a way that may influence other's voter's ballots, or to insert more than one ballot, they have misused their privilege and have thus, committed an insider attack.

The set of all voting system insiders is bounded, countable, and well-defined. That is, there are a limited number of insiders, they are enumerable, and given an arbitrary entity, we can systematically determine if that entity is an insider or not by answering the question: "Does the entity have at least one intended privilege that can impact an electoral outcome?".

A comprehensive discussion of the reasons that a trusted entity might become a traitor is beyond the scope of this paper. However, one simple explanation is that a [malicious] individual that is interested in one or more elected offices may choose to infiltrate the electoral process with the intent of acquiring electoral privileges in order to misuse them to impact their contest of interest. Similarly, rather than personally infiltrating the electoral process, the malicious entity may enlist a friend or family member that has needed privileges, and they become an insider/traitor.

Finally, we define a *voting system insider attack* to be any attack on a voting system that leverages misuse of privileges by an insider. Attacks that do not leverage intentional privilege misuse by an insider are outsider attacks.

1.2. Insiders Acting as Outsiders

It is important to recognize that an insider need not misuse their privilege in order to attack a voting system. For example, a poll worker that is a voting system insider may attack the voting system by delaying mail delivery in an attempt to have otherwise valid ballots disqualified because they are delivered to the LEO after the legal deadline for acceptance. Even though that attack may be carried out by an insider, it did not involve misuse of privilege, and for that reason, we consider it an outsider attack.

1.3. Outsiders Cannot Act as Insiders

Some argue that outsiders become insiders if they are able to maliciously attain privileges. In our model, we specifically bind insider status to intentional trust. Under this distinction, we consider malicious trust acquisition as masquerading and, for example, consider identifying masqueraders as an approach to defend against outsider attacks. Accordingly, while insiders may accomplish outsider attacks, under our definitions, outsiders can only participate in insider attacks if they collude with an insider that misuses privileges.

2. Voting System Insider Acts and Actors

The definitions and model presented in the first section form the theoretic core of our paper. The ability that they allow to identify insiders and combat insider attacks is our most critical result.

In this section, we identify categories of voting insiders and give our classification assignment. The categories are based on generic voting system functions, which we describe first. We then identify the actors that accomplish the functions that justify their voting system insider status.

2.1. Acts: Voting System Functions

While elections have some asynchronous aspects, for the most part, the election process is serial and synchronous, both for the act of voting and for the process of conducting the election. For that reason, we present the voting system functions generally in the order they occur, beginning with formulating elections policy and ending with storing voting systems between election cycles. We identify authority that is necessary to accomplish the general functions, but leave detailed descriptions to the later section where we will identify which actor's needs specific privileges.

2.1.1. Formulate Elections Policy

Conducting elections is a fundamental government responsibility that is shared by local, state, and federal agencies. The U. S. constitution assigns the responsibility for federal elections exclusively to the states, though it allows for federal governance and assistance under unusual circumstances. Two primary federal agencies with direct electoral responsibilities are the Federal Elections Commission that focuses on federal elections law oversight and elections funding and the U. S. Elections Assistance Commission that is concerned with operational elections' aspects. Each of these agencies has privileges that can impact electoral outcomes. Similarly, the U. S. Department of Justice has oversight responsibility for federal law and is in a position to influence electoral outcomes at the federal, state, and local levels.

Secretaries of State most often oversee state electoral responsibilities. Secretaries of State are responsible for elections in all but a few states and within that office there is usually a senior elections director whose sole responsibility is elections management and oversight. States generally delegate responsibility for conducting elections to localities, so state official's participation is largely relegated to policy establishment, oversight, and conflict resolution. It is usually the Secretary of State that certifies results for state and federal offices and that conducts recounts and audits when they are required.

State judiciary may become involved in electoral issues before, during, and after the voting period. Their impact can be pivotal in election outcomes, so their participation in election issues is always sensitive. While their impact on election policy is less visible than their involvement at the decision end, the impact on policy has equal potential for decisive impact.

Local Elections Officials (LEO) are, in many ways, the main officials that are responsible for planning and carrying out elections. They establish local policy, acquire elections equipment, identify and arrange polling locations, train poll workers and voters, and conduct other activities necessary to carry out fair and accurate elections.

2.1.2. Configure Voting Systems for Operation

Elections are complex processes that require extensive preparatory activity. Once the policies are in place, the process is clear, the equipment is purchased, and the many other long term resources are in place, the planners are ready for an election. As election date approaches, LEOs take actions to activate the

election. Officials train and assign poll workers, formulate ballots, arrange for necessary printing, ensure that computing resources are properly prepared, and conduct other activities necessary to ensure that that the voting system is prepared to deliver the proper ballot to each voter that chooses to vote and that their selections will be accurately recorded and counted.

2.1.3. Collect votes

When people think of elections, they probably think of their own voting experience and how easy it is. They may stop in to their local polling place, mark their ballot, drop it in the ballot box or feed it into the scanner, and be merrily on their way. Total duration of the voting experience: 10 minutes. Or they may request an absentee ballot, mark it in the comfort of their home, and return it to their LEO well ahead of election day.

Few voters understand the complexity and magnitude of effort necessary to allow their voting experience to be so comfortable, while also ensuring electoral integrity. Poll workers must arrive early, polling places must open on time, printed materials must be accurate and ready to distribute, and computing resources must operate as they were designed, tested, and implemented. Absentee ballots must be properly handled multiple times. These processes depend on well-trained officials making good decisions as situations change and as the unexpected happens.

2.1.4. Transport Election Materials, Including Voted Ballots

Physical security is essential for many election components. Unsupervised access can allow malicious parties to undetectably corrupt election results. Election materials can be exposed to unsupervised accessibility at many points in the elections process. While voter education materials and unmarked ballots can be compromised

2.1.5. Tabulate results

After the voting period ends, the results are accumulated. The focus shifts from poll workers assisting voters in the polling place to poll workers turning over voted ballots, partial results, and other critical data to elections officials. This must be done in a way that ensures sufficient confidence that the results are accurate in order to certify them by the lawful deadline.

2.1.6. Confirm results

Election decisions are, for the most part, hierarchical in four levels: the Polling place, the Electoral Jurisdiction, State Elections Officials, and Federal Officials.

Precincts or polling places report results to the jurisdictional authority, usually the LEO, and the LEO reports results to state elections officials. State elections officials then certify results for their state and federal offices and report federal results through established reporting channels. Insiders are involved in the reporting process at each of these levels.

Conflicts must be reconciled at every level. Polling place officials review records and logs to ensure that they are providing accurate information to their LEO. LEOs reconcile inconsistencies before reporting to state officials and state officials reconcile conflicts before reporting results through established federal channels. At each level, conflict resolution may involve records reconciliation, audit, or full scale investigation before the selected individual is seated by the house for which they were competing.

At the extreme, the judiciary may be involved in electoral conflict resolution. Judiciary involvement can be triggered by law suits filed by voters, candidates, political parties, or other authorities.

Finally, for federal elections, responsibility for seating in the U. S. Senate and House of Representatives is exclusively theirs. That is, Congress itself decides who its members are. Though rare, there are instances of contests that have triggered Congressional investigation into a contest. These investigations may involve internal (Congressional) review or investigation by another government agency such as the General Accounting Office [e.g. see 1, 2]. On at least one occasion, the House of Representatives decided to seat other than the state certified selection.

2.1.7. Run for Office

Candidates are much more than names on lines on a ballot. As contestants, they have primary legal standing for judiciary action in elections. For many issues, they hold exclusive standing.

2.1.8. Vote

While candidates most directly feel the impact of electoral results, it is the voters that ultimately decide, or at least are intended to decide, the fate of the candidates. Voters are granted privileges to access voting systems and may participate in official election observation, in electoral audits and investigations, or in post-election judicial actions.

2.1.9. Operate facilities

In any election there are many organizations and individuals are granted privileges that have the potential of maliciously impacting electoral results. Facilities operators are one such example.

Depending on local procedures, facilities operators may have unsupervised physical access to sensitive records or equipment that record, store, or involved in reporting electoral results. Their compromise could result in allowing an attacker to maliciously alter or control an electoral result.

Facility owners and managers for local elections officials, polling places, voting system vendors, and voting system storage facilities all have privileges that, if misused, can compromise election integrity.

2.1.10. Manage Voting System Storage

A second generic set of service management positions that have relevant privileges are those that manage voting system storage during non-election periods. These personnel may have physical access that is similar to facilities managers and the impact may include altering or controlling electoral results.

2.2. Actors: Voting System Insiders

We now turn our attention to identifying actors that are likely to fit our definition of voting system insiders.

2.2.1. Elections Officials

Local Elections Officials (LEOs) may have the most trusted access of anyone. They interpret and implement state election policy and dictate local election policies and procedures. They impact voting system design, configuration, operation, tabulation, reconciliation, close out, and inter-election storage. Absent local controls, the LEOs privilege can be unbounded and her voting system-relative authority can be essentially unilateral.

Beyond the influence of the principle, there are many LEO subordinates that enjoy substantial important privileges. For

example, members of the LEO Technical Staff may have unsupervised access to voting systems or to the software that controls or interacts with them. Similarly, contracted elections consultants may require privilege to devices and software.

Due to their intermittent temporal nature, LEOs leverage employment of temporary elections staff members during election operations. These temporary officials may have access to, or be able to influence, voting system configuration information, voting systems themselves or the software that they execute, or other documents or resources that can impact election integrity.

Maybe the most recognizable elections officials are polling place staff who are dominantly volunteers that are paid a pittance for their efforts and may be most accurately described as temporary workers.

The two primary impacts of state elections officials are for policy establishment and as conflict arbiters. The former can create electoral properties that may tend to favor one style of campaign tactics over another, one political party over another, or even one candidate over another.

As high level policy makers, federal officials electoral impact is generally strategic. Their decisions determine issues such as Voluntary Voting System Guidelines 3], usage of federal voting system funding, etc. There decisions impact broad electoral properties rather than any specific contest.

2.2.2. Executive Branch Authorities

The Federal Executive Branch has two primary avenues to affect elections. First, the policy actions taken by the FEC and EAC can impact electoral outcomes. Additionally, the U. S. Department of Justice can trigger civil and criminal action, either as part of an oversight effort or in response to citizen complaints.

At the state level, the Secretary of State is the final arbiter on many electoral outcomes and on other issues that can substantially impact election integrity and public perception.

Finally, local executive branch involvement is usually limited to mayoral participation in elections official funding request decisions.

2.2.3. Legislative Branch Authorities

As was earlier noted, federal legislative authority is powerful, but limited. While the houses of Congress are the final arbiters of their membership, they have little immediate impact on other contests. As policy makers, they can strategically impact elections even though they have no direct electoral responsibilities.

Examples of federal forays into elections policy include the Help America Vote Act of 2002 [4], the Uniformed and Overseas Citizens Absentee Voting Act [5], and the Military and Overseas Voter Empowerment Act of 2009 [6]. Congressman Rush Hold of New Jersey has repeatedly introduced legislation that calls for federal elections to be conducted on voter marked paper ballots. These legislative initiatives are attempts to create a national remedy for perceived deficiencies in state election policies and processes, but little is known of their partisan impact.

Because of the constitutionally dictated state elections authority, state legislatures have more direct impact on elections than their federal counterpart. They can dictate voting system standards, or even specific voting system products, to local elections officials.

2.2.4. Judicial Authorities

As is intended in federal and state constitutions, the judiciary has equal and opposite power relative to initiatives taken by the executive and legislative branches. That is, the judiciary at each level holds the power to overturn legislation and executive directives if they are judged to violate constitutional principles.

However, the greatest power held by the judiciary is the ability to arbitrate elections disputes. The now infamous Florida Supreme Court decision to change election law during the 2000 presidential election [7] demonstrated the judiciary's power to influence electoral outcomes.

Similar to the federal judiciary, state justice officials are also often in a position to influence electoral outcomes. Consider, for example, the June 6, 2010 primary election in Riverside, California [8]. In that election, some 12,600 bundled absentee ballots were delivered to elections officials some three hours after the legal deadline. Approximately 40 days later, well after the electoral results were announced, the district judge ruling in a lawsuit filed by the California Secretary of State directed that those late-arriving, illegal ballots be counted. While there have been no credible claims that the decisions by the Secretary or by the judge were biased by the electoral outcome, the potential for such mischief is self evident.

2.2.5. Candidates

As noted above, contestants have legal standing to not only contest results, but to contest ongoing election processes before, during, and after the voting period. In many cases, they are the only entity that has standing to trigger certain levels of review, particularly judicial review.

Even before election day, they have access to processes that qualify or disqualify voters and that can significantly impact election results. Candidates have standing to engage elections officials, legislators, and the judiciary regarding ballot design, voting procedures and elections audits. Like any other privileges, these privileges can be misused.

2.2.6. Auditors

There is presently inertia in the election integrity community[2] and among some among elections officials, to dramatically expand reliance on audits to verify election accuracy. Unfortunately overlooked in this otherwise sound approach is the vulnerability that audits may introduce into the electoral process.

While election fraud has traditionally involved actions taken during the voting period, information about the electoral outcome can trigger and facilitate post voting period fraud [9]. This gives auditors privileges that solidify their status as voting system insiders.

2.2.7. Voting System Developers

The inevitable emergence, and controversial expansion, of vendors into elections operations introduces a new and sometimes unrecognized vulnerability into the elections process. Because of the nature of software, it is very difficult to detect additional functionality that may accomplish malicious purposes [10]. Thus, developers may be able to introduce backdoors, logic bombs, and

[2] See e.g. http://www.electionaudits.org/

other malicious code into voting system code that can facilitate attacks once the system is implemented.

Clearly, being temporally, logically, and physically close to the election allows an attacker to have more detailed information and to more precisely target any intended impact. Developers are logically separated from the elections that they support. Developers do not know contests, let alone candidates, that their software will support. Thus, their targeting must be strategic, which is fundamentally different than an attacker that aims to influence a voting system during the voting period.

2.2.7.1. Original Development

Candidates are rarely, if ever, known when election software is originally developed. Thus, in order to impact a specific election, or elections in general, a malicious programmer may either need to use the information that they have or simply install a logic bomb or backdoor access point.

For the former, a developer would generate an attack based on generic information that they know about the election process. For example, they know that in U. S. federal elections, candidates are usually affiliated with a political party. Thus, a malicious developer may resort to inserting malicious code that favors a particular political party, e.g. by flipping every 100th vote for any candidate in party A to the candidate for party B.

On the other hand, a developer may insert malicious code that can allow them to gain "backdoor" access to program execution at any time in the future. Once election details were known, the attacker would use the backdoor to access the machine and insert malicious code that accomplishes a specific election attack.

2.2.7.2. Maintenance Programmers and System Integrators

Maintenance programmers may employ the same generic strategies as original developers, but have two additional capabilities. First, maintenance programmers may know many details about an upcoming election that they could use to influence an election to their advantage. For example, they may know who likely candidates are in most of the contests or they may even be able to project reasonable approximations of the expected ballot styles for the upcoming election. Second, maintenance programmers may have physical access to voting systems and direct access software and configuration files during logic and accuracy testing or even during the voting period.

2.2.7.3. Voting System Integrator

In some instances, an electoral jurisdiction may engage a system integrator to comprehensively implement an existing voting system in their election structure. For example in 2008, Finland contracted a company to implement another vendor's voting system in a remote voting pilot [11].

Often, such arrangements require that significant privileges be granted to the integrator, possibly equivalent to the developer and to operational personnel, which can create a particularly vulnerable security situation.

2.2.7.4. COTS Vendor

COTS vendors are further removed from elections than even developers, so their attack pathway must be even more generic. The most likely approach for a COTS vendor that desires to influence elections would be to provide a backdoor that could be exploited during the voting period.

2.2.8. Building Manager, Owner and Maintenance Staff

As noted earlier, many attacks are enabled or facilitated by gaining unsupervised physical access to elections offices, polling places, voting system storage locations, etc. Because of their ownership or supervisory authority, building managers often have approved, or unapproved, privileges that allow them such access to any elections-related space. Cleaning staff canonically represent this insider threat.

Conversely, an attacker that gains malicious access without abusing privilege, e.g. by breaking in to a warehouse where voting systems are stored, is not a voting system insider.

2.2.9. Voting System Storage Inventory Managers

Inventory managers may have unsupervised physical access, similarly to that of building managers, to voting systems during their transport and storage and their potential impact is similar.

2.2.10. Voters

It may seem unusual that we consider voters as elections insiders. Voters are the system end users, while insiders are often exclusively considered to be people that develop or execute the system. Both consistency and accuracy dictate otherwise.

Voters are granted a variety of privileges that are not granted to non-voters and that can be misused to maliciously, and dramatically alter electoral outcomes. First, for a limited period of time voters are granted physical access to voting machines, often with limited or no supervision. During that access period, a malicious voter may tamper with the voting machine, e.g. by inserting a removable media device that allows them to install malware on that voting machine. If one machine is successfully infected, that malware could propagate to most, or even all voting machines within the jurisdiction [12]. It could spread to other jurisdictions if machines or media are shared across jurisdictions.

Second, voters often interact with other elections systems, including voter registration systems, absentee ballot requests systems, etc.

Finally, voters are eligible to become poll workers and may be actively involved in election management.

In our model, ineligible voters that are able to maliciously acquire valid voter credentials are considered to be outsiders.

Voting System Threat Taxonomy

2.3. Voting System Attack Types

In its primitive form, a vote is simply data to the voting system and while there are an infinite number of different types of attacks on voting systems, the impact of most voting system threats falls into the three data management categories of ADD, CHANGE, and DELETE (ACD). For example, the canonical Ballot Stuffing attack simply adds illegal votes into the "vote database". Vote flipping is comparable to a database change operation, while deleting votes is, well, you get the point.

While most voting system threats types may be categorized as add, change, or delete votes, there are attacks that do not fit well into any of those categories. For example, a software attack that predetermines the total vote outcome by altering the accumulated result in an electronic voting machine may be represented as a series of ACDs, but its essence is the threat against vote accumulation, rather than against individual votes.

2.4. Threats by Function

It may seem to many citizens that elections administration is only required every other year because federal elections dominate electoral news coverage. In reality, the voting period is merely one task in a life cycle that repeats itself often throughout the year, every year.

Threats change throughout the election life cycle. For example, Denial of Service threats are most common during the voting period while Accumulation threat opportunities mostly occur during canvass, recount, and audit functions.

In this section we briefly describe the electoral functions and map them to insiders that may pose electoral threats. Our function descriptions are generic and we recognize that the election cycle and the related terminology vary substantially across the country.

2.4.1. Voting System Development

There is an inherent risk that voting system developers may incorporate subtle, malicious features in a voting system that can be used to create bias in the outcome of elections conducted on those systems. Examples of the types of features that can create systematically predictable impacts may include, for example:

(a) Creating a type of interface that may be unnecessarily difficult for a particular demographic group to understand.

(b) Inserting logic that omits a candidate from a targeted political party, dependant on a variety of related factors.

The proliferation to, and dependence on, computers in the electoral process dramatically expands the threat surface to developers. Because of the nature of software systems developers could embed malicious "backdoors" that could allow them to include detailed attack information during a specifically targeted election with a reasonably low risk of being detected.

2.4.2. Election Configuration

In this function, elections officials identify the races to be contested, enroll candidates, create ballots, print necessary materials, and prepare machines for election day. There are many vulnerability points that occur during election configuration. Two key areas are (1) Ballot creation and (2) Logic and accuracy testing. Both represent attack surfaces for insiders that are conducting those functions and for developers and system integrators that have, or had, access to the internal process logic.

2.4.3. Voting Period

The voting period is well-understood for its opportunity for electoral mischief that includes a myriad of voting system attacks.

2.4.4. Precinct Closeout

Immediately after the voting period ends is a particularly vulnerable time for two reasons:

(1) The accumulated results become available to elections personnel

(2) Source data must be moved from the polling place to secure storage

2.4.5. Accumulation at the Local Jurisdictions

After the voting period, the election process and artifacts are canvassed by local elections officials. First, the jurisdictions gather the information from the polling places, ballot collection points, absentee ballot storage, and other sources of voter selection information. They then began accumulating and verifying the electoral results for each of the contests that is involved in the election.

Once the source documents are collected, the tabulation is complete, and inconsistencies are reconciled, the results are presented to the elections board by the senior elections official in the jurisdiction, and the result is certified for presentation to the state.

Elections are particularly vulnerable during the local verification function because an attacker may target either the source documents, the tabulation results, or a combination of the two. Moreover, each of these are in transit at some point, often from remote regions, transported by volunteers potentially in their personal vehicles.

2.4.6. State Accumulation

State certification follows a pattern that is similar to the local jurisdictions' canvass. Data is collected and accumulated, incorporating the results from the various jurisdictions, and a tentative result is formed. The process and results are reviewed, potential errors are investigated, and the final result for each contest is decided.

Once state elections officials have accomplished their accumulation, verification, and reconciliation processes, the state certifies the results for state and federal elections.

2.4.7. Post Certification Audit

At the conclusion of the accumulation function some states perform a post-election audit. While these audits are not routinely used to determine electoral outcome, they may be used for that purpose and thus offer an attack surface for malicious parties.

The audit may be so simple as a re-verification of the electoral records of voter logs, voter registration systems, provisional ballots, handling of absentee ballots, etc.

They may be more sophisticated and include statistical audits that use a randomized algorithm to select precincts or jurisdiction wide polling locations for comprehensive audit.

2.4.8. Contest Periods

At essentially any time during the election process, candidates, voters, or other parties may access the court system to influence the electoral process or some electoral result. The most familiar such law suits are filed during and after state accumulation, usually in federal elections. In some states, there is an official "contest period". We refer here to the generic meaning of the term as being the time at, or after, state certification when candidates and other parties with appropriate standing may file suit to challenge an electoral process or outcome.

The contest period offers a critical threat surface because insiders know exactly how many votes need to be altered in order to change the outcome. Thus, even a small change may be sufficient to steal the election.

2.4.9. Retrograde and Storage

After the election is over, the results are reported, and the data is gathered, the elections equipment and materials must be stored so they are available for use in a future election cycle. While retrograde and storage is a straightforward task in most cases, during these activities, the machines and the materials that

support the election are often in transit and subject to various types of harmful access by unauthorized persons.

One vulnerability that may be exploited through this type of unofficial access is the opportunity for installation of malicious software. If the equipment and resources are improperly accessed, e.g. by building managers, during storage, that can pose a threat to election integrity for the next election cycle. For this reason, whether these materials and machines are stored in city, county, or contracted storage facilities, they must be protected from unauthorized access.

2.5. Insiders' Opportunity by Election Function

It is instructive to consider who the prospective insiders are in each electoral function and which function offers vulnerability to each prospective insider. We summarize the insider-function correlation in Table 1. Our categorization is not absolute; rather, we focus on the most likely opportunity for each insider. Additionally, a single entity could bridge the category borders by acting in multiple insider categories in the same election, e.g. as a voter and an executor (e.g. a poll worker).

We now amplify a few of the less obvious Table 1 connections.

Let's first address the policy maker impact. A malicious policy maker could propose and promote election policy at the federal, state, or local level that could influence voting system properties in a way that would favor a particular political party.

Table 1: Insider Threats by Electoral Function

	Voting System Development	Election Configuration	Voting Period	Precinct Closeout	Local Accumulation	State Accumulation	Contest Period	Retrograde and Storage
Developer	X	X	X	X				
Policy	X	X	X	X	X	X	X	X
Configurator		X	X		X		X	
Executor	X	X	X	X	X	X	X	X
Candidates		X	X		X			
Voters			X					
Judiciary	X	X	X		X		X	X
Bldg Mgr		X	X	X	X		X	X
Supply Mgr		X					X	X

Consider, for example, a proposed policy to leverage technology that could improve electoral access for military members. If a legislative member has data that convinces them that military voters will systematically support candidates from the opposing political party, they may oppose use of any technology that expands access to that group on [disingenuous] technological grounds.

The prospective policy impact spans all electoral functions, including when polling places are opened, the mechanisms that voters may use at the polling place, absentee ballot requirements, the local and state accumulation processes, and how contested results are resolved.

The other entity with broad and deep privileges that offer powerful options to an insider are Local Elections Officials or LEO's. LEO's (termed "executors" in Table 1) have deep influence on every aspect of the electoral process, including influencing voting system development decisions.

Those that configure elections (configurators) can have their greatest impact during the voting period. However, because of their access to equipment, they may be able to influence accumulation and verification procedures by installing malware that alters results or contradicts earlier reported results.

3. Conclusion

Insider attacks are particularly insidious threats to electoral integrity. Traitors that misuse the trust that is placed in them often have system access that facilitates malicious acts and their subsequent cover-up efforts. There is a long history of insider attacks on elections in the United States.

In this paper, we precisely define what it means to be an insider and we identify several classes of elections insiders. We also categorize the threats that each insider class has relative to the electoral functions.

We address several insider categories that are rarely, or never, mentioned in considering election insider threats. For example, we have not previously seen members of the judiciary identified as prospective elections insiders and we give a concrete example of how judges can accomplish insider attacks on elections. Similarly, we identify the impact that policy makers can have on the electoral process and show how malicious legislators may be able to influence a broad spectrum of elections through the laws that they propose and promote.

Insider attacks are real and imminent threats to electoral integrity and to the foundational democratic processes that public elections support. By identifying insiders and categorizing the threats that they pose allows us to create policies and procedures that better ensure sound elections and to ensure the integrity of our way of government at local, state, and federal levels.

Bibliography

[1] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, “Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, Final Report”, SAIT Laboratory, Florida State University, February 23, 2007, http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf.

[2] GAO-08-425T, Elections: Results of Testing of Voting Systems Used in Sarasota County Florida's 13th Congressional District, Nabojyoti Bakakati, U. S. Government Accounting Office, http://www.gao.gov/new.items/d08425t.pdf

[3] United States Election Assistance Commission, "Voluntary Voting System Guidelines (VVSG)", www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx

[4] Public Law 107-252, "Help America Vote Act of 2002", 107th Congress, USA

[5] U. S. Public Law 99-410, "The Uniformed and Overseas Citizens Absentee Voting Act", August 28, 1986

[6] Military and Overseas Voters Empowerment (MOVE) Act, Attached to the 2010 National Defense Authorization Act (H.R. 2647), 2009

[7] Supreme Court of Florida, "Stay Order, CASE NOS.: SC00 2346, 2348 & 2349," , Friday, November 17, 2000, http://jurist.law.pitt.edu/election/00-2348stay.pdf

[8] Jim Stark, "Judge: Court will not disenfranchise 12563 voters; hearing on uncounted ballots ends", July 9, 2020, http://www.instantriverside.com/2010/07/judge-court-will-not-disenfranchise-12563-voters-hearing-underway-on-uncounted-ballots/

[9] Alec Yasinsac and Matt Bishop, “The Dynamics of Counting and Recounting Votes”, IEEE Security and Privacy Magazine, May-June 2008, Volume: 6, Issue: 3, pp. 22-29

[10] K. Thompson. "Reflections on Trusting Trust," Communications of the ACM, 27(8):761–763, Aug. 1984. Also in ACM Turing Award Lectures: The First Twenty Years 1965-1985, Copyright 1987 by the ACM Press and Computers Under Attack: Intruders, Worms, and Viruses Copyright, Copyright 1990 by the ACM Press. http://www.acm.org/classics/sep95/.

[11] John Ozimek "Finland's flawed e-voting scheme - blame the voters?" The Register, Nov. 9, 2008, http://www.theregister.co.uk/2008/11/09/finland_evoting/

[12] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, “Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, Final Report”, Security and Assurance in Information Technology Laboratory, Florida State University, February 23, 2007, see Appendix B, http://election.dos.state.fl.us/reports/pdf/FinalAudRepSAIT.pdf