Voting Systems Insiders and Insider Attacks

Alec Yasinsac
University of South Alabama
Mobile, Alabama USA

Abstract

Electronic voting systems are an integral element of our nation's infrastructure, providing the platform upon which we elect our local, state, and federal representatives. Those that develop, maintain, field, and operate voting systems are a primary threat to this infrastructure

Insider attacks are insidious threats to electronic voting systems. Traitors that misuse the trust that is placed in them often have system access that facilitates malicious acts and subsequent cover-up efforts. We define what it means to be an insider and precisely define an insider attack.

Elections are security-critical information systems that are highly susceptible to insider attacks. We identify classes of elections insiders and categorize threats that insider classes have relative to electoral functions. Beyond specifying well-known elections insiders such as poll workers and local elections officials, we address the enduring impact of system developers, operators, and maintainers, as well as several insider categories that are rarely, or never, mentioned in considering election insider threats.

We do not claim that insider attacks are the only threats to elections nor can that controlling insiders by itself, makes elections safe. However, insider attacks are imminent threats to electoral integrity. Identifying insiders and categorizing the threats that they pose allows us to create policies and procedures that better ensure sound elections.

Keywords: Security Models, Election Threats, Voting System Security, Secure Software

1. Introduction.

Electronic voting systems are an integral element of our nation's infrastructure, providing the platform upon which we elect our local, state, and federal representatives. Those that develop, maintain, field, and operate voting systems are a primary threat to this infrastructure. Elections are security-critical information systems that are highly susceptible to insider attacks [1]. Elections officials are the canonical "insider" in the electoral process. They operate and oversee elections based on the policies and procedures that they created. Those are the perfect combination of authority that can facilitate undetected electoral tampering.

As elections become increasingly automated, the opportunity for mischief by computer programmers and operators similarly expand. Their impact may be even broader than that of

elections officials because software malice may spread across jurisdictions or even across states and may endure for years through many election cycles.

In this paper, we detail the acts and actors that constitute insider attacks on voting systems. We discuss the prospective impact of software developers, system integrators, and technologists that maintain and operate voting systems as persistent voting system insiders. We also evaluate the breadth and depth of impact of the canonical insiders (elections officials) and introduce classes of insiders that may not have been previously considered (the judiciary, legislative bodies, et al.)

1.1. Insider Attack Defined

We consider an attack to be any action that is intended to violate the voting system's security policy. In practice, many election 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.

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. Thus, an insider attack must involve misuse of the granted privilege by the insider in order to violate a security policy. That is, the trusted entity becomes a *traitor*. The set of voting system insiders is always countable and well-defined, i.e., those given

intentional trust are enumerable and given an arbitrary entity, we can systematically determine if that entity is a voting system insider or not by answering the question: "Does the entity have at least one intended privilege that can impact an electoral outcome?"

Finally, we define a *voting system insider attack* to be any attack on a voting system that leverages misuse of privileges by an insider. E.g. a cryptographic key-holder that uses their key to divulge election results prior to their legal announcement would be an insider attack. Similarly, a building key holder that uses their key to alter election documents kept under lock and [their] key the night before the election is also an insider attack.

1.2. Traitors and Intruders

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 practical result. From a security standpoint, because insiders are intentionally trusted parties, their identity is always known to the privilege grantor. The “insiders list” can be important information in forensic efforts. Moreover, we prefer to prevent and deter insider attacks as a class, rather than in detail, which is impossible if the “insider” and “outsider” classes merge. Thus, we reject the notion that outsiders may become insiders via malicious activity.

Misuse of intended trust is the essence of being an insider, aka. *a traitor*. Trusted individuals not only hold special privileges, but also hold special responsibilities not just to protect the rightful application of that trust, but also to protect against perceptions of its misuse. In that sense, trust is a position of honor and violating trust is, in some sense, more heinous than the intended malice alone. Moreover, the access that insider status grants may offer opportunity for greater impact for less effort than for their malicious outsider counterparts.

We 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 outsiders, aka. *intruders*. Accordingly, while insiders may accomplish outsider attacks, under our definitions, outsiders can only become insiders by attaining intended trust.

2. Voting System Insiders

In this section, we identify categories of voting system insiders and give our classification assignment justifications. 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 insider status. A summary of voting system actions and actors is provided in Figure 1.

Voting System Actions	Voting System Actors
Formulate Elections Policy:	Federal, State & Local officials, Advocacy Groups, Vendors
Configure Voting Systems:	Elections Technical Staff, Vendors
Collect Votes:	Elections Officials
Transport Election Materials	Elections Officials (permanent or temporary)
Run for Office:	Citizens
Tabulate Results	State, Local Officials
Confirm Results:	Federal, State, Local Officials & Judiciary
Vote:	Registered Voters
Operate facilities	Various
Manage Voting System Storage:	Non-elections Staff

Figure 1. Voting System Acts and Actors

2.1. Canonical and Non-Canonical Voting System Functions

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

Conducting elections is a fundamental government function that is shared by local, state, and federal agencies. The U. S. constitution assigns elections responsibility to the states, though it allows for federal governance and assistance under unusual circumstances. The two primary federal agencies with 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 elections' operational aspects. Each of these agencies has privilege that can impact electoral outcomes. Similarly, the U. S. Department of Justice has oversight responsibility for all federal law and is in a position to influence electoral outcomes at the federal, state, and local levels.

Secretaries of State are responsible for elections in all but a very few states and within that office there is a senior elections director whose sole responsibility is elections manage-ment 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 the Secretary of State that certifies results for state and federal offices and that conducts recounts and audits when required.

State judiciary may become involved in electoral issues before, during, or 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 of policy has equal potential for decisive impact.

Local Elections Officials (LOE) are 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 other activities necessary to conduct fair and accurate elections.

Elections are complex processes that require extensive preparation. Once policies are in place and the process is clear, equipment is purchased, and the many other long term resources are in place, the planners are ready for an election. As election approaches, LOEs prepare 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.

When people think of elections, they probably recall the ease and simplicity of their own voting experience. Few voters understand the complexity and magnitude of the 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. These processes depend on well-trained officials making good decisions as situations change and as the unexpected happen.

There are many, varied aspects to electoral integrity, e.g., physical security is essential for many election functions. Unsupervised access to elections equipment or materials can allow malicious parties to undetectably corrupt election results. Election materials can be exposed to unsupervised access at many points in the elections process. Protecting voted ballots during transit is particularly critical to election integrity.

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 that must attain sufficient confidence that the results are accurate in order to certify them by the lawful deadline.

Election organization is generally hierarchical in four levels (where necessary):

1. Polling place
2. Electoral Jurisdiction
3. State Elections Officials
4. Federal Officials

Precincts or polling places report results to the jurisdictional authority, usually the LOE, and the LOE reports results to state elections officials. State elections officials then certify results for their state and federal offices and report federal results through appropriate channels.

Results must be validated, and conflicts reconciled, at every level. Polling place officials review records and logs to ensure that they are providing accurate information to their LOE. LOEs 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.

At the extreme, the judiciary may be involved in electoral conflict resolution. Judiciary involvement can be triggered by law suits filed by voters, candidates, or political parties. When law suits occur, they are always partisan and are usually controversial, resting virtually all trust on the judiciary to conduct a comprehensive, unbiased resolution process.

Finally, for federal elections, seating in the U. S. Senate and House of Representatives is reserved exclusively to the legislative bodies themselves. That is, Congress itself decides who its members are. Thus, there are rare 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 2,

3]. On at least one occasion, Congress seated other than the state certified candidate [4, See McCloskey, 1984].

Candidates are much more than names on a ballot. As contestants, they have access to critical election processes and procedures and also hold primary legal standing for judiciary action in elections. For many issues, they hold exclusive judicial standing.

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 often granted trusted privileges to access voting systems and may participate in official election observation, in electoral audits and investigations, or in post-election judicial actions.

In any election, there are many organizations and individuals that have administrative and management access 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 are 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. A second generic set of service management positions that have relevant privileges are those that manage voting machines and auxiliary equipment storage through non-election periods. Personnel that conduct these activities may have physical access that is similar to facilities managers and the impact may include altering or controlling electoral results.

2.2. Prospective Voting System Insiders

We now turn our attention to identifying actors that are allotted trust in the voting process, i.e. prospective voting system insiders. These insiders fit nicely into the three categories of governmental insiders, system developers, and voters.

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 his voting system-relative authority can be essentially unilateral.

Beyond the influence of the LEO, there are subordinates in the elections office that enjoy important trusted 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 election's intermittent nature, LEOs leverage employment of temporary elections staff members during election operations. These temporary officials may have trusted 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 predominantly volunteers or that are paid a nominal amount for their efforts.

While local elections officials have broad and deep impact on election integrity, state officials are generally limited to the two primary impacts of policy establishment and conflict arbitration. The former can create electoral properties that, for example, may tend to favor one style of campaign tactics over another, one political party over another, or even one candidate over

another. The latter may offer advantage to one party over another in close elections. At the state level, the oft Governor-appointed Secretary of State is the final arbiter on many electoral outcomes and on other issues that can substantially impact election integrity and public perception.

As high level policy makers, federal officials' electoral impact is generally strategic. Their decisions determine issues such as Voluntary Voting System Guidelines [5], usage of federal voting system funding, etc. There decisions impact broad electoral properties rather than any specific contest, but their privileges are no less trusted than state and local elections officials. The Federal Executive Branch has little electoral involvement beyond the policy actions taken by the FEC and EAC.

Federal legislative authority over elections is powerful, but limited. While the houses of Congress are the final arbiters of their membership, they have little immediate impact on other contests. Still, 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, the Uniformed and Overseas Citizens Absentee Voting Act, and the Military and Overseas Voter Empowerment Act of 2009. Congressman Rush Hold of New Jersey has repeatedly introduced legislation that calls for federal elections to be conducted on voter marked paper ballots. Such 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.

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 if it is adjudicated to violate constitutional principles. 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". However, the greatest power held by the judiciary is the ability to arbitrate elections disputes. The now infamous Florida Supreme Court decision to alter election law during the 2000 presidential election [6] demonstrated the judiciary's power to directly 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 [7]. 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.

As noted above, candidates 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.

There is presently inertia in the election integrity community 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 voting process, where auditors become trusted insiders. While election fraud has traditionally involved actions taken during the voting period, it is well known that information about the electoral outcome can trigger and facilitate post voting period fraud [8] by auditors with partisan, malicious intentions.

The inevitable emergence, and controversial expansion, of computers 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 [9]. Thus, developers may be able to introduce backdoors, logic bombs, and other malicious code into voting system code that can facilitate attacks once the system is implemented.

Clearly, being close to the election temporally, logically, and physically avails the attacker to more detailed information and to more precisely target any intended impact. Developers are separated from the elections they support in all three of these spheres. They do not know which contests, candidates, or issues that their systems will support. Thus, their targeting must be different than an attacker that aims to influence a voting system during the voting period.

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

backdoor access capability. 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 50th vote for candidates 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.

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

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 [10]. Such arrangements may 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.

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 to influence elections is to provide a backdoor that can be exploited during the voting period.

Many software attacks are enabled by gaining unsupervised physical access to elections offices, polling places, voting system storage locations, etc. Because of their supervisory authority, building managers often have approved, or easy but unapproved, privileges that allow them such access to elections-related space. Cleaning staff canonically represent this insider threat, but plumbers, electricians, and managerial staff may also have privileged physical access that could allow them to install malware into voting machines or computers used for accumulation. Inventory managers may have unsupervised physical access, similarly to that of building managers, to voting systems during their transport and storage.

The insider status of voters is somewhat less clear, but is maybe more illuminating than for LOEs. It may seem unusual that we consider voters as elections insiders. Voters are the end users, while insiders are often thought to be people that operate the system or its underlying components. However, voters are granted a variety of privileges that are not granted to non-voters that can be misused to dramatically, maliciously alter electoral outcomes.

For example, in virtually all cases, voters are granted physical access to voting machines, in some cases 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 [2] and to other jurisdictions if machines or media are shared across jurisdictions. Second, voters are often involved 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.

3. Software and Computing Threats to Voting Systems

Voting systems may be viewed as nothing more than information systems where a vote is simply data to the voting system. While there are an infinite number of different types of attacks on voting systems, the impact of many voting system threats falls into the three data management categories of add, change, and delete against one or more votes on one or more ballots. For example, the canonical Ballot Stuffing attack adds illegal votes into the vote count. Vote flipping is comparable to a database change operation.

The proliferation 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.

In this section, we identify computing functions where developers, maintainers, configurators, and operators may leverage insider trust to attack elections. Our descriptions are generic and we recognize that the election cycle and that terminology differs substantially across the country.

3.1. Voting System Development, Configuration, and Operation

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. The types of features that can create systematically predictable impacts may include:

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 being displayed on the ballot, dependent on a variety of related factors.

Prior to Election Day, elections officials identify the races to be contested, enroll candidates, create ballots, print necessary materials, and prepare machines for voting. There are many vulnerability points that occur during election configuration. Two key areas are ballot creation and logic and accuracy testing of the computing equipment. Each of these areas represents attack surfaces for insiders that are conducting those functions and for developers and system integrators that have, or had, access to the equipment or the software's internal process logic.

3.2. Voter Qualification: Registration Databases, Authentication, and Authorization

Identifying and qualifying voters is a fundamental election function that depends heavily on computers and is, thus, a critical component of E-Voting. Voter registration information is entered, validated, and stored on computers before the election and voter rolls are prepared so that voters can be authenticated and authorized to vote their ballot. Because the voter rolls are pivotal to the election process, they may be a target for a sophisticated intruder.

Beyond the simple attack of a registrar tampering with individual registration records, in many administrative environments, it would be simple for a trusted employee to insert removable media into a registration system computer and upload malicious software. This software could add records to the voter rolls that could allow illegal voters to cast ballots on Election Day. Similarly, the malicious software could delete records in order to disenfranchise legitimate voters of the opposing party. A more subtle attack may be to alter bits of identifying information about targeted voters in order to force them to vote via a provisional or challenged ballot. Alternatively, malicious software in the registration system could cause intermittent outages that will lengthen lines and frustrate voters in an attempt to drive down participation in targeted areas.

3.3. Voting Machines

The voting period is well-understood for the opportunity for electoral mischief that includes virtually all well-known types of voting system attacks. Vote flipping, denial of service, ballot manipulation, ballot injection, and accumulation compromise are examples of the attack types that occur during the voting period.

There are many studies that document security challenges in electronic voting machines, e.g. [11]. We illustrate the types of attacks on Direct Recording Electronic (DREs) voting machines that have no paper record that corresponds to the electronic ballot.

Malicious software may alter or replace electronically stored vote counts on the voting machine. Even if the voting machines record multiple copies of the cast votes, malicious software can control all electronic copies. Many of these attacks would need to be accomplished by those involved in managing the voting functions: elections officials and poll workers. For paper-based voting system, ballot stuffing is a well-known attack type. Conversely, with electronic voting systems, developers may have set an attack in place within the elections software.

3.4. Tabulation, Accumulation, and Auditing

Altering accumulation data is a high impact objective, e.g.a software attack may predetermine the total vote outcome by altering the accumulated result in an electronic voting machine during the poll closing process. Precinct closeout is particularly vulnerable 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

Once source documents are collected, tabulation is complete, and inconsistencies are reconciled, results are presented to the elections board by the senior elections official in the jurisdiction, and the result is certified to the state. Elections are particularly vulnerable during the local

verification function because an attacker may target source documents, electronic tabulation results, or a combination of the two. Attacks have been demonstrated against computers shortly after they are powered off [12]. Moreover, much of the voting day product is in transit at some point, often from remote regions, transported by volunteers in their personal vehicles.

At the conclusion of the accumulation function, some states perform a postelection 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 as simple as a re-verification of the 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 audits.

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. Malicious software, installed on computers that either were involved in the election or that are exclusively used in the audit, may be used to change electoral results. Alternatively, electronic attacks may be used to raise doubt about the final result for future political advantage. Even the appearance of malicious software on any elections related computer can be used to raise doubt, e.g. see [13].

4. Conclusion

The U. S. government is implemented through a distributed elections process that comprises a pivotal element of our critical infrastructure. Without electoral integrity, we cannot expect our representative system of government to work as it was designed and intended. 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 U.S. elections and electronic voting expands the threat surface and increases the prospective impact for insider attacks.

In this paper, we identify several classes of election 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, e.g. 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 could influence a broad spectrum of elections through the laws that they propose.

Insider attacks are real and imminent threats to electoral integrity. By identifying insiders and categorizing the threats that they pose we can create policies and procedures that better ensure sound elections and protect the integrity of our way of government.

5. Acknowledgments

Thanks to Matt Bishop and David Dill for illuminating conversations regarding voting system insider threats. An early version of this paper appeared in the 2010 Workshop on Governance of Technology, Information, and Policies [14].

6. Bibliography

[1] Kocher, P. (2004). Insider risks in elections. Communications of the ACM, 47(7), 104.

[2] 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, http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf.

[3] 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

[4] Charlie Cook, “Close Races Spotlight An Ugly, Broken Mess,” The Cook Political Report, http://www.cookpolitical.com/node/2462

[5] U. S. Election Assistance Commission, "Voluntary Voting System Guidelines", www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx

[6] 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

[7] 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/

[8] 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

[9] K. Thompson. "Reflections on Trusting Trust," Communications of the ACM, 27(8):761–763, Aug. 1984. Also appears 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/.

[10] 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/

[11] Ryan Gardner, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, “Software Review and Security Analysis of the Diebold Voting Machine Software”, Final Report For the Florida Department of State, July 27, 2007, http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf

[12] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten, “Lest We Remember: Cold Boot Attacks on Encryption Keys”, Proc. 17th USENIX Security Symposium (Sec ’08), San Jose, CA, July 2008.

[13] www.computerworld.com/s/article/9019560/Worm_attacked_voter_database_in_notorious_Florida_district

[14] Alec Yasinsac, "Insider Threats to Voting Systems," Workshop on Governance of Technology, Information, and Policies (GTIP), December 7, 2010