Threats to Voting Systems

Douglas W. Jones
University of Iowa

A position paper for the NIST workshop on Threats to Voting Systems
October 7, 2005, Gaithersburg, MD

Abstract

A public catalog of threats to voting systems should be created. While such a catalog may help educate attackers, it is essential to a reasoned public debate about the adequacy of our voting system standards, the adequacy of our recommendations for best practices and the adequacy of state laws and administrative rules. If we can quantify the costs of threats and defensive measures we will be able to rank order threats in order of their likelihood and defensive measures in the order of their importance, but such quantification will be difficult. We must be careful to avoid giving the impression that our threat catalog is complete, or that addressing all of the threats in the catalog is sufficient to absolve vendors or election officials from responsibility for the failures of their systems.

A Catalog of Voting System Threats is not a Threat

When asked about the vulnerabilities of their voting systems, many election officials will simply deny that their voting system has vulnerabilities. Others will refuse to answer, saying that discussions of this topic are inappropriate. The most frequently cited reasons for a refusal to discuss this subject are:

1) Public discussion of this subject could enable election fraud.

2) Voter confidence is essential to the legitimacy of elections, and public discussion of this subject is a threat to voter confidence; therefore such discussion is a threat to the legitimacy of elections.

3) After having spent millions of dollars on this voting system, a public admission that the system is less than perfect would invite questions about the propriety of this expenditure.

Curiously, the answer to the first objections was stated well over a century ago, in a book edited by Charles Tomlinson.[1] There, of course, the question was "whether or not it is right to discuss openly the security or insecurity of locks." The book offers the following answer:

> Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done. If a lock, let it have been made in whatever country, or by whatever maker, is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance.

There is no doubt that rogues have been corrupting scattered elections across the

United States for two centuries. Joseph Harris devoted Chapter IX of his landmark 1934 book to this topic, clearly documenting numerous cases of fraud and providing a useful list of types of voting fraud.[2] Edmund Kallina's study of the 1960 election in Chicago shows that the kinds of irregularities documented by Harris continued with little change 30 years later.[3] While the technology has changed, and while we may be doing somewhat better today, there is no reason to believe that the rogues have lost interest.

Questions 2 and 3 rest on the same questionable ethical premise: That it is better for the public to remain ignorant of the shortcomings of their government or their voting system than it is to encourage open public discussion of such issues. While there may be some short term benefit of suppressing debate, in the long run, such suppression can only lead to an uninformed electorate making uninformed decisions. That is certainly a threat to our democracy.

Organizing a Threat Catalog

In any discussion of threats to voting systems, the list of possible threats can grow quite unwieldy. Even the short list of threats identified by Harris shows evidence of this (See Chapter IX of [2]):

1) Registration frauds.
2) Repeating (individual voters voting more than once).
3) Ballot box stuffing.
4) Chain ballots.
5) Voter assistance.
6) Intimidation and Violence.
7) Altering Ballots.
8) Substitution of Ballots.
9) False Count and False Returns.
10) Altering Returns.

Here, we find chain voting, a very specific and somewhat technical vote buying attack, listed on a par with voter assistance, a broad general category of attack. We can clearly sort the different approaches to election fraud according to several different criteria.

Before continuing with an enumeration of these criteria, it is worth noting the distinction between threats to a voting system and attacks against that system. In general, attacks are deliberate malicious acts, while the term threat is broader, encompassing accidents and mistakes.[4] An old maxim in the area of computer security is clearly applicable here: Almost everything that a malicious attacker could attempt can also happen by accident; for every malicious attacker, there may be thousands of ordinary people making ordinary careless errors. We are equally concerned by errors and by attacks, so we will use the term threat except where deliberate malice is necessarily involved.

What phase of the voting process is being manipulated. Most of Harris's taxonomy addresses this. Generally, an adversary can attack the system in one or more of the following phases:

1) Registration
2) Polling place access (intimidation, violence, destruction and vandalism).
3) Voter manipulation (repeat voting, chain voting, voter assistance).
4) Ballot manipulation prior to tabulation (substitution, stuffing, counterfiting).
5) Threats to the ballot tabulation process itself.
6) Threats to the results of the tabulation process.

All of the threats identified by Harris can be fit into this scheme, and if we set out to produce a master catalog of voting system threats, this appears to be a reasonable top-level organization for a threat taxonomy. An expanded version of this taxonomy is given in the appendix. There is good reason, however, to provide secondary indices into the threat catalog that support alternative taxonomies.

What technology is vulnerable. Certain threats are technologically neutral, while others target specific technologies. Configuration file manipulation can only be used to attack voting systems that have configuration files, while chain voting is only possible when voters are allowed to handle physical ballots.

Who carries out the attack. Everyone involved in the election, whatever their role, has an interest in the outcome, and everyone can make mistakes. While many people are involved, they can be classified into a few basic roles, and it is not difficult to identify, for each attack, the role of the initiator(s) and the roles from which participants must be recruited.

1) Individual voters.
2) Outside attackers, including hackers, precinct captains and others.
3) Polling place workers and other temporary election staff.
4) Permanent employees at the election office.
5) Election officials.
6) Equipment vendors.
7) Policy makers.

Matters of scale. Retail fraud involves small-scale tinkering, where a separate act is required for each illegally obtained vote. Most fraud committed by individual voters is in this category. Wholesale fraud is at the other extreme, where a single act can change the outcome of an entire election or even of all elections from then on. Adoption of discriminatory policies by the government represents the most extreme form of wholsale election manipulation, although the very word fraud is problematic in the context of immoral legislative acts.

Possible Refinements to the Threat Catalog

In its simplest form, a threat catalog consists of an enumeration of the threats to the voting system, with clear documentation of each threat. The description should be complete enough to allow evaluation of whether a particular voting system is adequately defended against that threat. In many cases, this level of completeness will not be sufficient to allow a potential attacker to carry out the threat, while in other cases, particularly for the nontechnical attacks, it will be difficult to avoid complete disclosure of the necessary details.

Many users of the catalog will need documentation, for each attack, of the defensive measures that can block or deter that attack. Some defensive measures are preventative, entirely blocking the attack if they are properly in place. Other defensive measures, such as post-election auditing, only allow detection of the attack. Some measures do not even guarantee detection, but merely create a risk of detection, and others merely raise the cost of an attack.

Some users of the threat catalog will prefer this simple presentation, where all information about a specific threat is consolidated in a single narrative description. On the other hand, some users of the catalog will notice that each individual attack or each error in the conduct of an election has structure. Each attack, or each error, involves the intentional or accidental exploitation of some set of vulnerabilities in the voting system. Many different attacks may exploit the same vulnerability.

Our threat catalog can be refined by identifying, for each attack, the set of vulnerabilities on which it rests, and then documenting the vulnerabilities.[4] Some attacks will rest on a single vulnerability, but others are more complex. Chain voting, for example requires obtaining a blank ballot, which may be done by exploiting any of a number of vulnerabilities, and then finding voters vulnerable to subversion, and then finding procedural vulnerabilities that allow those voters vote a different ballot than the one they were issued at the polling place.

By splitting attack descriptions from vulnerability descriptions, we can produce attack descriptions that are far more compact, but they will also be far less readable and they may be harder to produce. This suggests that the refined catalog should be a secondary document, but it is worth noting that the exercise of extracting vulnerabilities from attack descriptions can itself lead to the discovery of other attacks.

If we include defensive measures in our catalog, these can form a third section, since some defensive measures, such as various forms of auditing, defend against multiple vulnerabilities, while other defensive measures apply only to one. As with vulnerabilities, consolidation of the discussion of a defensive measure in one place will allow more complete discussion of that defense, but it also makes it more difficult for a reader to quickly determine which combinations of defenses will guard a particular voting system against a particular attack.

Using the Catalog

Threat catalogs can be used in a variety of ways. If we classify attacks according to the voting technology to which they apply, we can easily extract from our catalog, for any voting system, the set of attacks an adversary might exploit in corrupting that system. This, of course, could be used by an adversary to design their attack, but it is also the list of attacks an election administrator must be prepared to defend against. If the threat catalog includes defensive measures for each threat or vulnerability, we can use it to assess election administration at several levels.

Evaluating the defenses of a particular voting system. We can evaluate a voting system, as used in a particular administrative context, against the threats listed in our catalog. To do this, we take the set of all defensive measures that surround that voting system and ask if that set includes at least one defense that will block each applicable threat. If we are serious about defense in depth, we should ask that each applicable threat be blocked by more than one defensive measure.

It is important to note, here, that each defensive measure can be classified as having technical and administrative components. One defense against chain voting, for example, uses numbered tear-off ballot stubs (See Chapter II of [2]). These are a technical component. These stubs, however, are of no value unless the polling place workers use them, and that use is the administrative part of the defense. Thus, we can say that a particular voting system is adequately defended if the following conditions hold:

1) The voting system mechanism must incorporate all of the technical components of the identified set of defensive measures. This should be insured by some combination of the voting system standards, state certification, pre-purchase product evaluation and post purchase retrofits.

2) The voting system must be administered in a way that incorporates all of the administrative components for the same set of defensive measures.

Evaluating the voting system standards. Given a threat catalog and a set of voting system standards, we can ask, for each class of voting systems governed by the standards, do those standards require the technical components of the defenses necessary to adequately block the applicable threats.

If the standards do not address some threat, this strongly suggests a weakness in the standards. If the standards require mechanisms that do not address some threat, then it is possible that some threat has not been identified that belongs in the threat catalog, but it is also possible that the the requirement itself is wrong.

It is worth recalling that our voting system standards have been developed with strong vendor input. Sometimes, this works to everyone's benefit, since the vendors are in contact with many potential customers and are sensitive to the real needs of those customers, but at times, vendors may attempt to manipulate the standards to their own advantage, inserting requirements for the purpose of limiting the competition. A well managed attack catalog can help us ferret out these spurious requirements, defending the standards against regulatory capture.

Evaluating the laws and administrative rules governing the conduct of elections. Given a threat catalog and the laws and administrative rules of a jurisdiction, we can ask, for each class of voting system permitted in that jurisdiction, whether those laws and rules require the administrative components of the defenses necessary to adequately block the applicable threats.

This is perhaps the single most valuable use for the threat catalog. In 1934, Harris pointed out that the laws governing the use of voting machines were, to a significant extent, being written by the vendors (See Chapter VII of [2]). In many cases today, it is difficult to ascertain what these laws mean or why some feature is required. Given a threat catalog as proposed here, we have some hope of answering these questions and arriving at a rational basis for evaluating these laws and evading regulatory capture.

It is, of course, essential that the defenses selected have the necessary technical support! Currently, there is an almost complete disconnect between the technical voting system standards and the drafting of law and administrative rules to govern the use of voting systems, and this leads to some very odd results where mechanisms are required to be present that are not permitted to be used or where procedures are required that are ineffective because the necessary mechanisms are not fully implemented.

While the NIST, TGDC and EAC have no direct authority in the setting of the state laws and administrative rules that govern the conduct of elections, they do have the charge to examine and promulgate codes of best practices in this area. Such a code could take the form of a model code of election law, following the path that Harris took in 1934 (See Chapter II of [2]). The problem with this is that there is huge variation from state to state in the way voting systems are governed. In some states, statutes are general and all specific details are relegated to administrative rules, while in other states, almost everything is spelled out in statute.

It would be very useful if each edition of the voting system standards were accompanied by a checklist of the administrative measures that are assumed to be present to complete the implementation for each defense incorporated into the technical standards. This checklist could be used in any jurisdiction to determine if the local voting system laws and administrative rules meet the assumptions made by the voting system standards.

The Possibility of Quantitative Evaluation

In the above discussion, the basic measure of adequacy was completeness of coverage. Either the defenses in place for a particular voting system covered the set of threats listed in the catalog, or some threats were not covered. Defense in depth was discussed only in terms of counting the number of defenses that were in place to cover each threat. No basis was given for assessing the likelihood of different attacks, nor was a basis given for assessing which defenses should be used when more than one attack is possible.

Assessing the likelihood of an attack. If we can determine the cost of overcoming the defenses that are in place to guard against each threat, we can assess which attack to expect from a rational and well-informed attacker. For any particular voting system in any particular administrative context, we should expect the least-cost attack while we may be able to largely ignore the more expensive attacks.

The problem we face in doing this is arriving at an estimate of the cost of overcoming each defense that is in place. Cost can be dollarized, it can be estimated in man-hours of effort, or it can be estimated in terms of the number of people required. Some of these costs will be easy to estimate, for example, the cost of cracking a well-chosen password by trial and error, while others are extremely difficult to estimate, for example, how much it would take to bribe a key person. To determine the cost of a particular attack, we must determine the cost of overcoming each defense, and then navigate a least-cost path through the set of defenses to mount the attack.

The fact that so many of the costs are fuzzy poses a serious problem. We can confront this problem by using perturbation analysis. To do this, we vary the cost estimates for each component of the attack over the reasonable range of values for that cost, and then examine how this influences the overall result. Having done this, we can now describe the cost of each attack with a range of values, and as a result, we may have not just one minimum-cost attack, but a set of attacks that are each potentially the minimum cost attack. This is basically a Monte Carlo method, but we can also accomplish much the same thing analytically using fuzzy math.

Assessing the cost effectiveness of various defenses. There are many threats that can be blocked by several different defensive measures, and many defensive measures are effective against several different attacks. It is natural to ask, in this context, which defenses we should implement.

Consider, for example, the problem of improving an inadequate set of voting system standards. The resistance to any broadening of the standards will typically depend on the cost, to the election administrators, of the new defensive measures required by that broadening. In order to defend a proposed broadened standard, it would be nice to be able to demonstrate that, among the defenses that could have been required, the new defenses that were required are the most effective, in the sense that no other set of defenses with comparable costs raises the cost of an attack as much.

Demonstrating this will require not only reasonable estimates of the costs of each attack in our attack catalog, but also reasonable estimates of the costs of each of the applicable defensive measures. These estimates will likely be as imprecise as the estimates of attack cost because there are few good studies of the actual economics of elections. The cost of voting system software is extraordinarily difficult to assess, and accurate measurement of the costs of defensive measures taken at the polling place has only rarely been attempted.

Conclusion

The development of a voting system threat catalog offers some immediate benefits. If we can document the known defenses against each threat, we can use it as a tool for evaluating the laws and regulations governing both voting equipment and the conduct of elections to see if these threats are adequately addressed. This can help us in the evaluation of voting system standards, best practices documents, and much more.

If we can produce reasonable estimates of the cost of each attack in the catalog, we may be able to produce a useful rank-ordering of the threats we ought to be wary of. If, in addition, we can produce reasonable estimates of the implementation costs for each defensive measure, we should be able to conduct cost-benefit analysis of the different defensive measures. The value of these quantitative assessments will depend on the precision of our cost estimates. It seems likely that the best estimates we will be able to make will be imprecise, which means that we will be able to offer only rough rankings of the various attacks and defenses.

There is one very serious risk in publishing a threat catalog that has not been considered here: That the catalog might be considered complete, and as a result, vendors and government officials might be absolved of responsibility for defending against any threats not documented in the catalog. If our threat catalog ever grows to the point that it appears to be exhaustive, this will become a very real risk. Any published version of the threat catalog must therefore begin with a disclaimer and a warning that someone, somewhere, may be hard at work devising new attacks on the machinery of democracy.

Acknowledgement

I would like to acknowledge the helpful suggestions of those who have read early drafts of this paper, notably Ronald Rivest and Eric Lazarus. NIST and NSF grant CNS-052431 provided partial support for the author's participation in the NIST workshop.

Notes

[1] A. C. Hobbs, *Locks and Safes*, Charles Tomlinson, ed., Virtue & Co., London, 1853.

[2] Joseph P. Harris, *Election Administration in the United States*, The Brookings Institution, 1934.

[3] Edmund F. Kallina, Jr. *Courthouse over White House -- Chicago and the Presidential Election of 1960*, University Presses of Florida, 1988.

[4] This distinction is commonly made in computer security texts; see, for example, Section 1.2 of Charles P. Pfleeger and Shari L. Pfleeger, *Security in Computing*, Prentice Hall. 2003. IEEE Standard 729 introduces similar distinctions in the terminology for discussions of quality control.

Appendix: An Expanded Threat Taxonomy

The following threat taxonomy is an expansion of the taxonomy given in the body of this paper based on phases of the election process. It is, at best, a preliminary work, and will almost certainly need revision as a result of finding threats that do not fit cleanly into it. On the other hand, the exercise of building this taxonomic tree has itself suggested a number of threats which might have been difficult to identify without this effort.

- 1) Registration
  - 11) One person registering in multiple places
  - 12) Registration of non-voters (such as dead people)
- 2) Polling place access
  - 21) Intimidation to prevent voting
    - 211) Intimidation outside the polling place
    - 212) Selective challenges to "undesirable" voters
  - 22) Violence to prevent voting
  - 23) Vandalism to prevent voting
    - 231) Physical destruction of voting equipment
    - 232) Tampering with equipment
      - 2321) Tampering with hardware
        - 23211) Substitution of improper mechanisms
      - 2322) Tampering with firmware
        - 23221) Substitution of improper code
        - 23222) Easter-eggs inserted by corrupt programmers
        - 23223) Trojans inserted into third-party components
        - 23224) Code injection attacks
      - 2323) Tampering with election configuration files
        - 23231) Substitution of media prior to installation
        - 23232) Alteration of contents of proper media
- 3) Voter manipulation

   31) repreat voting (note connection to category 1)
      311) voting under an assumed identity
      312) voting using illegal registration
   32) chain voting
   33) improper assistance to voters
      331) improper instruction given outside of voting booth
      332) improper advantage taken of voters with legitimate need for assistance
      333) voter requests assistance in order to earn reward from assistant
4) Ballot manipulation prior to tabulation
   41) ballot box stuffing
      411) stuffing before the polls open
      412) stuffing during voting
      413) stuffing after the polls close
   42) ballot alteration
      421) alteration of individual ballots
         4211) alteration prior to tabulation
         4212) alteration during tabulation ("short pencil" methods)
      422) substitution of counterfeit ballot box for authentic box
   43) challenging the authenticity of legitimate ballots
5) Threats to the ballot tabulation process itself
   51) announcement of tabulation result ignoring actual ballots
   52) uneven criteria for accepting votes depending on who is voted for
      521) threshold of acceptability depends on candidate
      522) threshold of acceptability depends on polling place
   53) incorrect counting
      531) counter overflow errors
      532) carry propagation errors
6) Threats to the results of the tabulation process
   61) substitution of counterfeit data
      611) substitution of counterfeit ballot box
      612) substitution of counterfeit tabulation results
   62) alteration of data
   63) rejection of legitimate data