Developing an Analysis of Threats to Voting Systems: Workshop Summary
Hilton Washington DC North Hotel , Gaithersburg, Maryland
October 7, 2005

FOREWORD

The Help America Vote Act (HAVA) of 2002 has given NIST a key role in helping to realize nationwide improvements in voting systems by January 2006. NIST research activities authorized by HAVA include the security of computers, computer networks, and computer data storage used in voting systems, methods to detect and prevent fraud, and protection of voter privacy and the role of human factors in the design and application of voting systems. Complete details of NIST voting research are available at http://www.vote.nist.gov.

The National Institute of Standards and Technology (NIST) hosted a workshop to allow the U.S. election community to participate in developing an analysis of threats to voting systems. The workshop took place on October 7, 2005, at the Hilton Washington DC North in Gaithersburg, Maryland.

The goal of the workshop was to solicit and gather threat analysis material and critical analysis of the collected threats; assess the plausibility of various scenarios and assumptions made; and extract lessons learned as a result of the analysis.

State and local election directors and officials, voting system security researchers, election lawyers, threat analysis experts, voting system vendors, and others from the public and private sectors submitted threat analyses of voting systems and participated in the workshop.

This workshop summary includes a synopsis of invited presentations and panel discussions as well as audience comments and questions. Audio recordings of the workshop proceedings served as the basis for panelist and presenter comments summarized herein. (Editor's note: Best efforts have been made to paraphrase the remarks of all participants. The positions expressed are solely those of the presenter, panelist, or audience participant. Full audio transcriptions of the workshop are posted at: http://vote.nist.gov/threats/audio.htm.)

Threat Analyses papers referenced in the workshop are included as an appendix. NIST encourages the election community to continue the threat analyses dialog begun at the October workshop. Papers and comments will be posted on the workshop web page: http://vote.nist.gov/threats/submissions.htm. Submissions can be made directly to voting@nist.gov.

TABLE OF CONTENTS

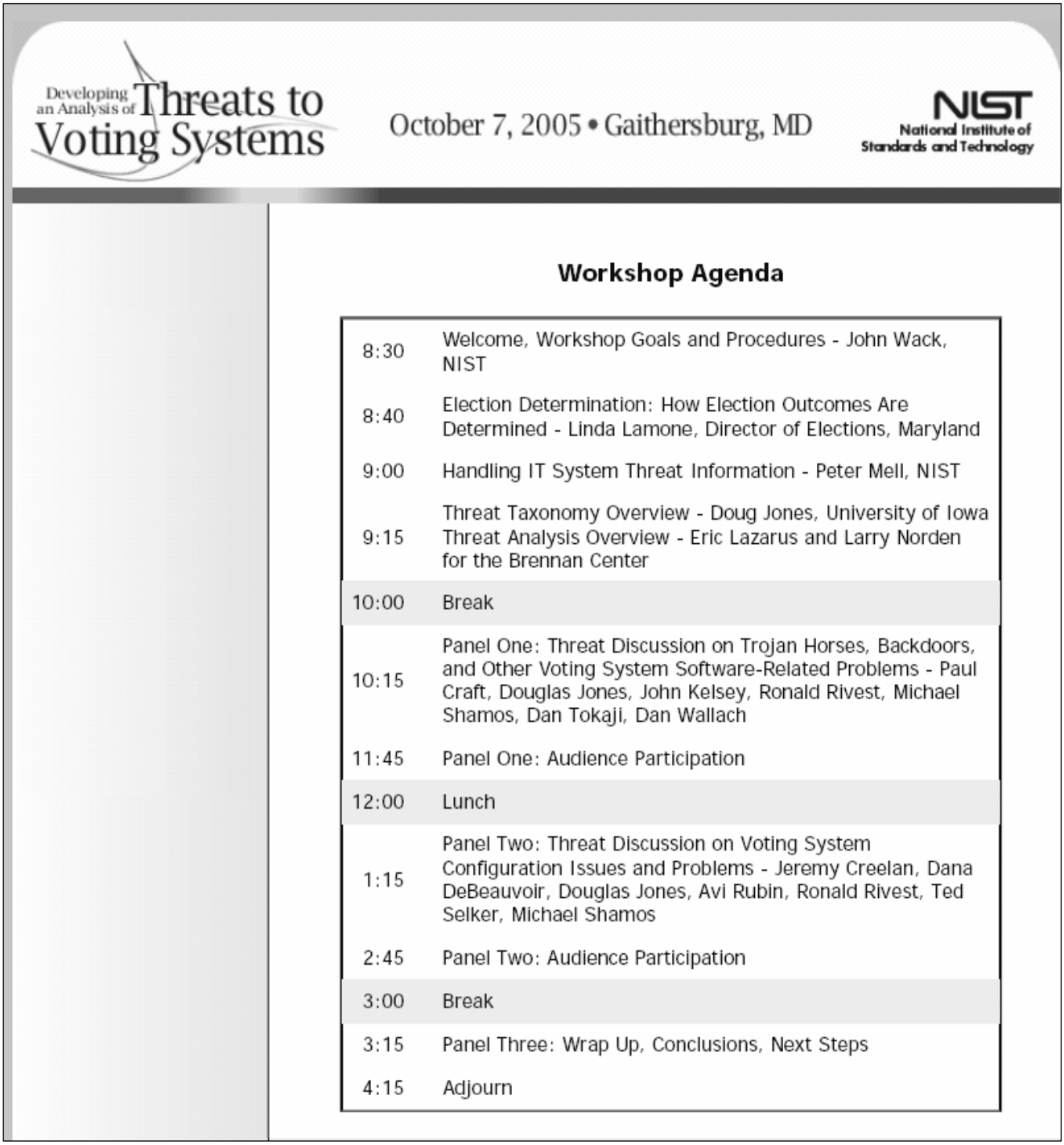
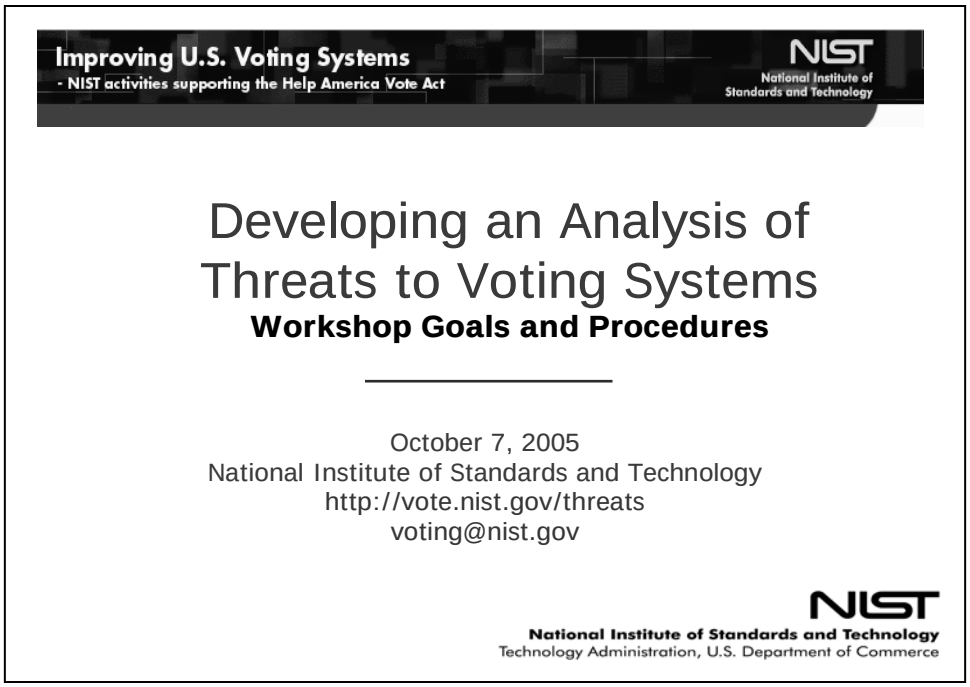

Developing an Analysis of Threats to Voting Systems
October 7, 2005 • Gaithersburg, MD
NIST National Institute of Standards and Technology
Workshop Agenda
8:30 Welcome, Workshop Goals and Procedures - John Wack, NIST
8:40 Election Determination: How Election Outcomes Are Determined - Linda Lamone, Director of Elections, Maryland
9:00 Handling IT System Threat Information - Peter Mell, NIST
9:15 Threat Taxonomy Overview - Doug Jones, University of Iowa Threat Analysis Overview - Eric Lazarus and Larry Norden for the Brennan Center
10:00 Break
10:15 Panel One: Threat Discussion on Trojan Horses, Backdoors, and Other Voting System Software-Related Problems - Paul Craft, Douglas Jones, John Kelsey, Ronald Rivest, Michael Shamos, Dan Tokaji, Dan Wallach
11:45 Panel One: Audience Participation
12:00 Lunch
1:15 Panel Two: Threat Discussion on Voting System Configuration Issues and Problems - Jeremy Creelan, Dana DeBeauvoir, Douglas Jones, Avi Rubin, Ronald Rivest, Ted Selker, Michael Shamos
2:45 Panel Two: Audience Participation
3:00 Break
3:15 Panel Three: Wrap Up, Conclusions, Next Steps
4:15 Adjourn

Figure 1



John Wack and Mark Skall, Information Technology Laboratory, NIST

As an introduction, John Wack of NIST's Information Technology Laboratory (ITL) reviewed the agenda for the workshop (Figure 1). He noted that the audience would have thirty-minute opportunities for participation after each panel discussion. Attendees were encouraged to ask questions and submit statements to the NIST web site.

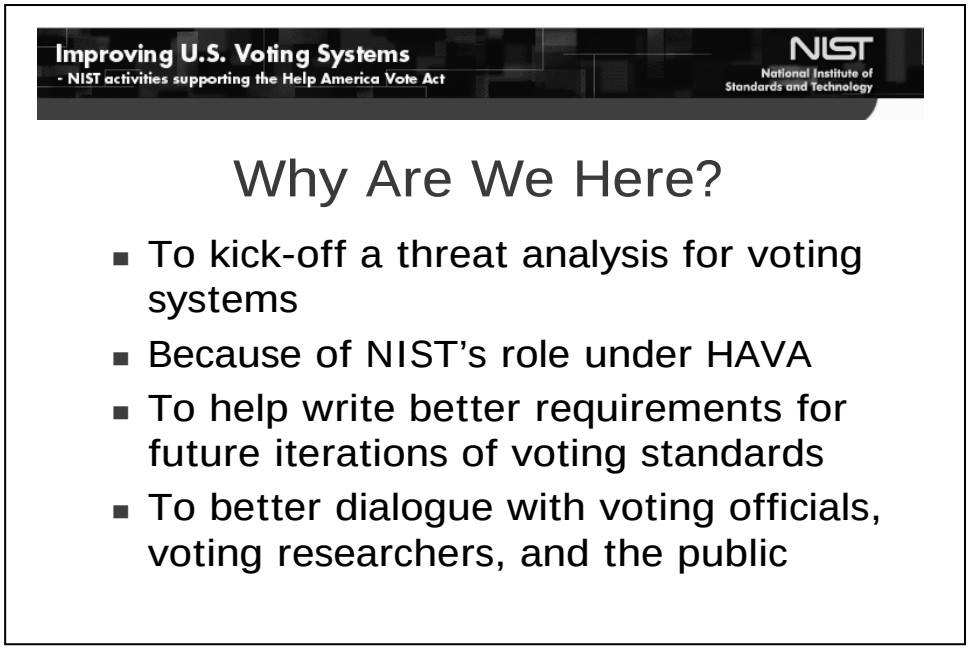


Figure 2

Mark Skall, Chief of ITL's Software Diagnostics and Conformance Testing Division, provided context for the workshop (Figure 2) and reviewed NIST's role under the Help America Vote Act (Figure 3). Specifically, NIST is engaged through the Technical Guidelines Development Committee (TGDC) in assisting the U.S. Election Assistance Commission (EAC) with technical guidance to write better requirements for future updates to the voluntary voting system guidelines (VVSG). A major element in the next iteration of the standards will be security requirements. It makes sense to define the problem before you engineer the solution. A threat analysis is a critical step towards defining the problem (Figure 4). Mr. Skall also noted that NIST and TGDC members viewed the workshop as a means to maintain a dialogue with the election community on threats to voting systems and to reach consensus where possible.

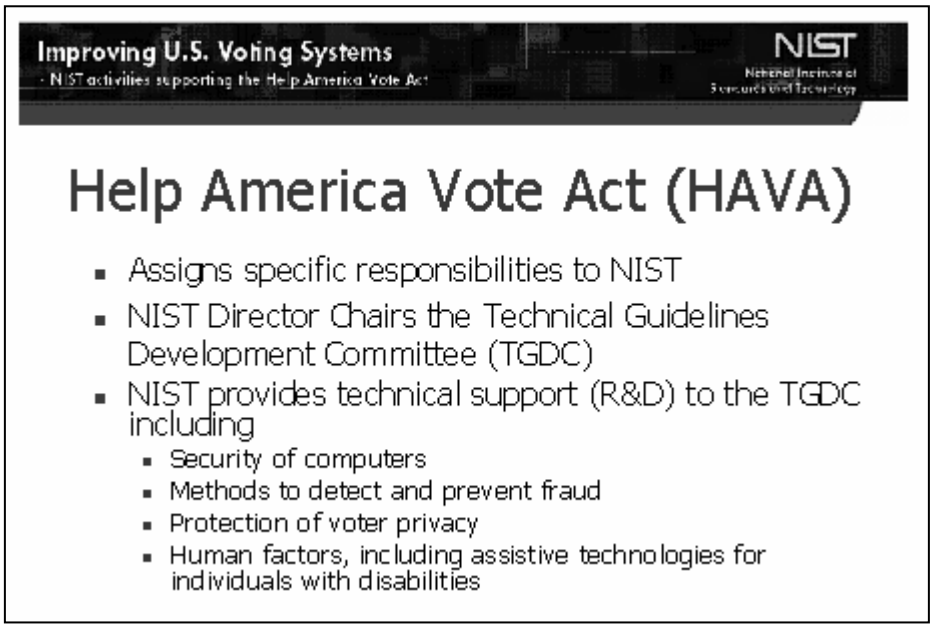


Figure 3

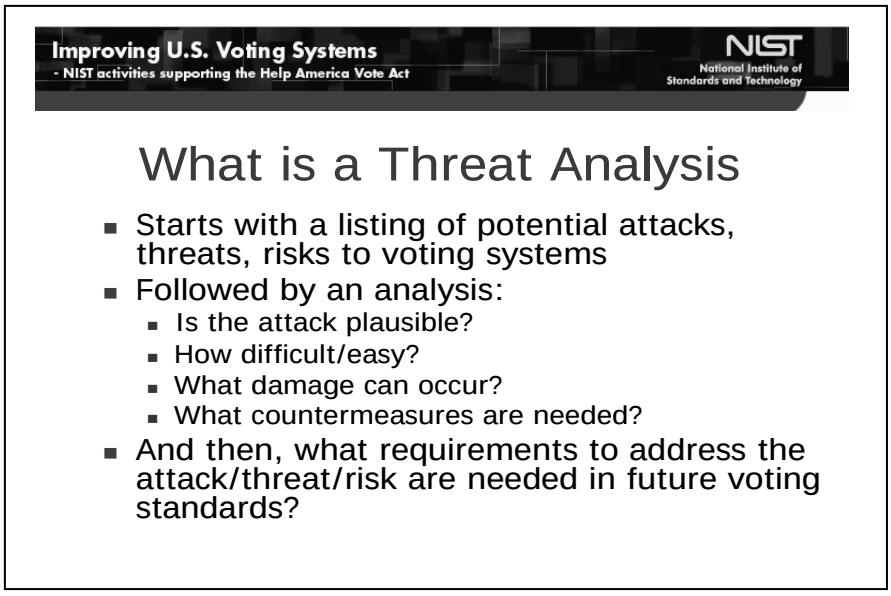


Figure 4

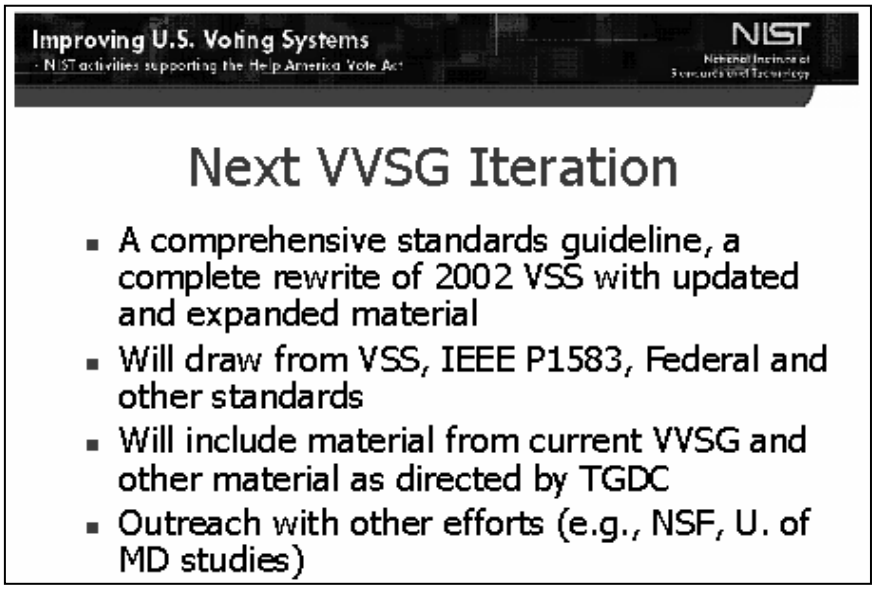
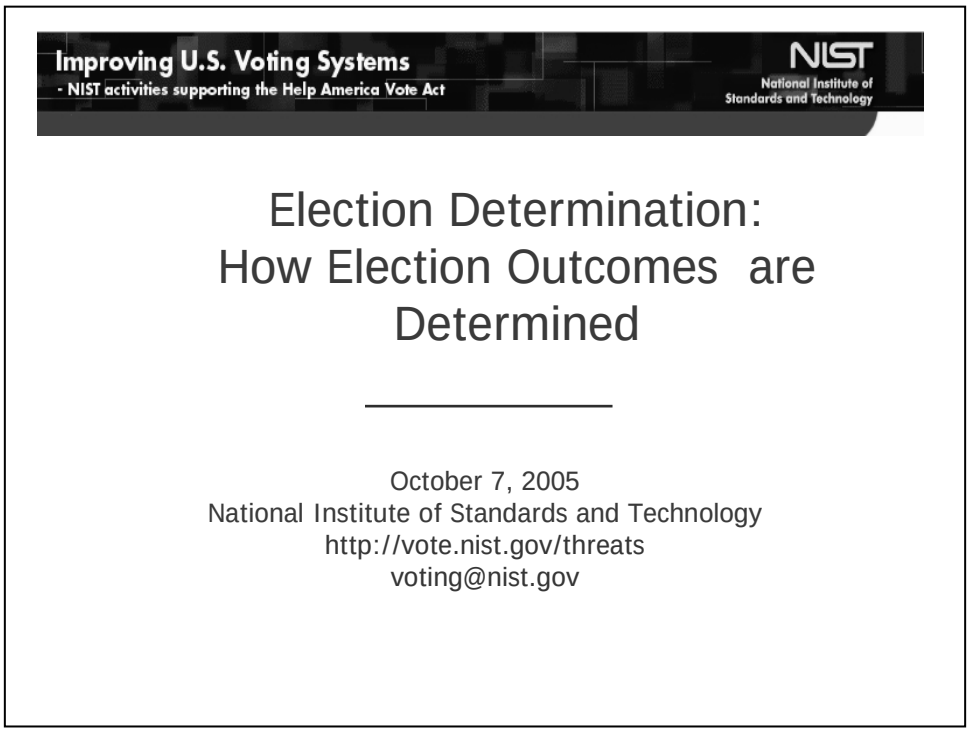


Figure 5

Mr. Skall noted that there was little time to engage in outreach to the election community during the development of the first iteration of the VVSG due to the strict time frame imposed under HAVA. NIST plans to engage in more comprehensive outreach with the development of the next iteration of the VVSG (Figure 5). Security requirements developed in the deliberative process of the TGDC may be onerous in terms of cost and time to implement. It will be important to inform the TGDC of the plausibility of threats. This threat analysis workshop begins that effort.



Linda Lamone, Director of Elections, State of Maryland; President, National Association of State Election Directors (NASED)

Ms. Lamone noted that the State of Maryland has entered into a contract with the University of Maryland Baltimore County (UMBC) Institute for Policy Analysis and Research to conduct a study of the Diebold voting systems in Maryland to determine whether additional security measures are required and whether additional verification methods are needed. The reason for the study is to provide state legislators with facts on which to base security decisions and not assumptions. Many security papers and analyses are based on assumptions and not facts. The goal of the academic study is a scientific result as well as policy recommendation for the state. Another outcome could be an academic center for the study of voting systems at the UMBC campus.

The State of Maryland voting system has undergone two comprehensive security studies as a result of a Johns Hopkins University paper on the voting system source code security weaknesses. The studies resulted in the implementation of a large number of new security measures. All of the changes are meant to ensure the integrity of the state's voting system. Parallel testing is now part of Election Day procedures as well as county logic and accuracy testing.

Maryland ensures that bipartisan election workers are part of the entire monitoring process with the voting systems. At the end of the day when the voting machines are closed down, the bipartisan workers sign printouts that indicate how many votes were cast on each machine. The

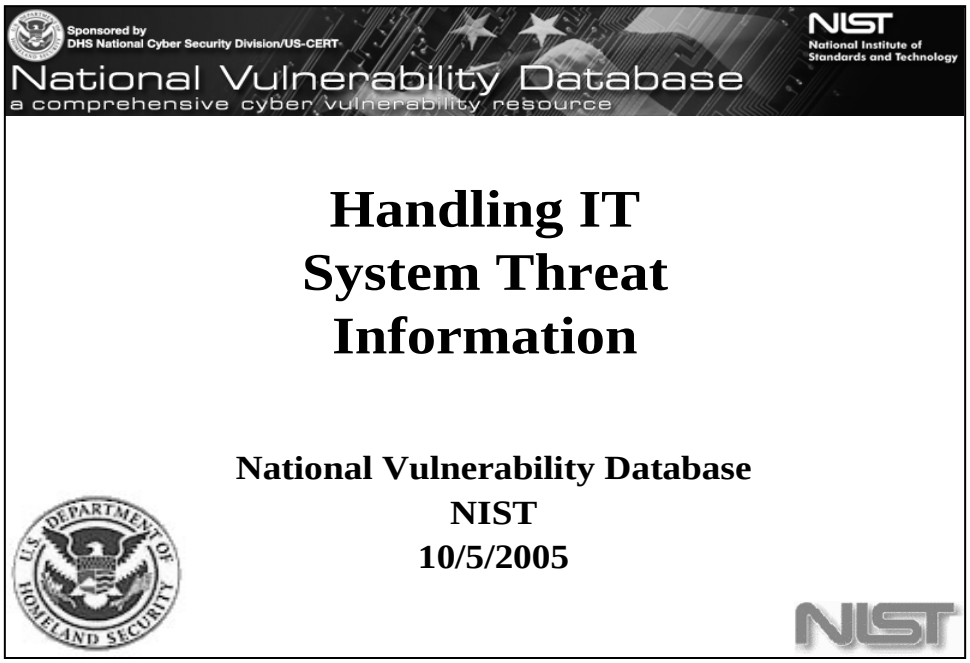
tapes and the zero count tapes are publicly posted usually the next morning. Some jurisdictions in Maryland accumulate the PC memory cards from each voting unit onto one unit to aggregate

the results and send them to the county office by modem. Data encryption protocols are used. Other jurisdictions have bipartisan poll workers remove the PC cards and physically drive them to the county election office where the results are accumulated. In either case, these “election night” results are unofficial.

Unofficial election results are accumulated because the media and candidates want them and they are posted on the state's public web page. State and local election officials ideally would like to wait until official election results can be tabulated, a process that extends from a few days to a few weeks. In Maryland, policies and procedures exist to ensure that the integrity of the (official) election results is maintained.

The morning after the unofficial election returns have been disseminated, one hundred percent of the voting machine's memory cards are re-read into the GEM server. The GEM server is programmed to know whether a memory card is correct or not through an electronic handshake. In addition, the absentee and provisional ballot count begins. An audit of the election takes place at this time as well. Since 2002, using the Diebold Direct Recording Electronic (DRE) voting systems, each audit has resulted in perfect matches between machine counters, PC cards, and voting day polling place registration records.

In conclusion, Ms. Lamone requested that the ensuing threat analysis discussions be factually based and not rely on assumptions. She also noted that electronic voting has been in use for many years in the United States without any documented instance of voting equipment failure. The documented failures within the voting process have been human failures.



Peter Mell, Director, National Vulnerability Database, NIST Computer Security Division

Mr. Mell first described the National Vulnerability Database (NVD), which contains all known computer security vulnerabilities and is available at http://nvd.nist.gov.

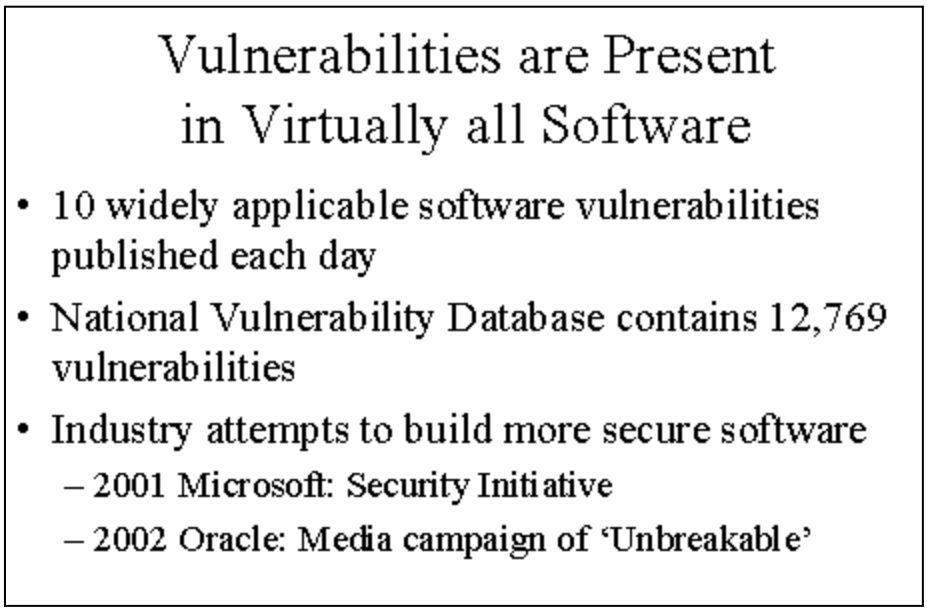


Figure 6

Mr. Mell noted that if you use software, vulnerabilities are likely to exist in that particular computer program (Figure 6). Vulnerabilities also exist in open source software products.

Software companies including Microsoft and Oracle have been working to deal with this difficult software security vulnerability problem. For example, Oracle has reduced their software vulnerabilities to twenty per year, which is noteworthy for a major software company.

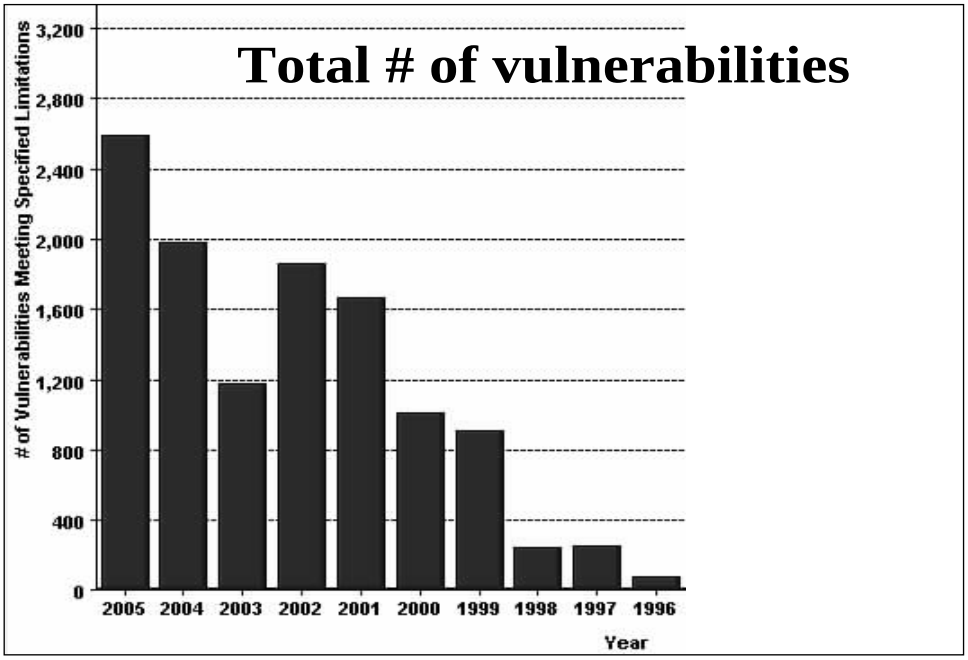


Figure 7

The number of vulnerabilities has grown nearly every year since 1996 (Figure 7). The reason for the anomaly in 2003 is not known at this time.

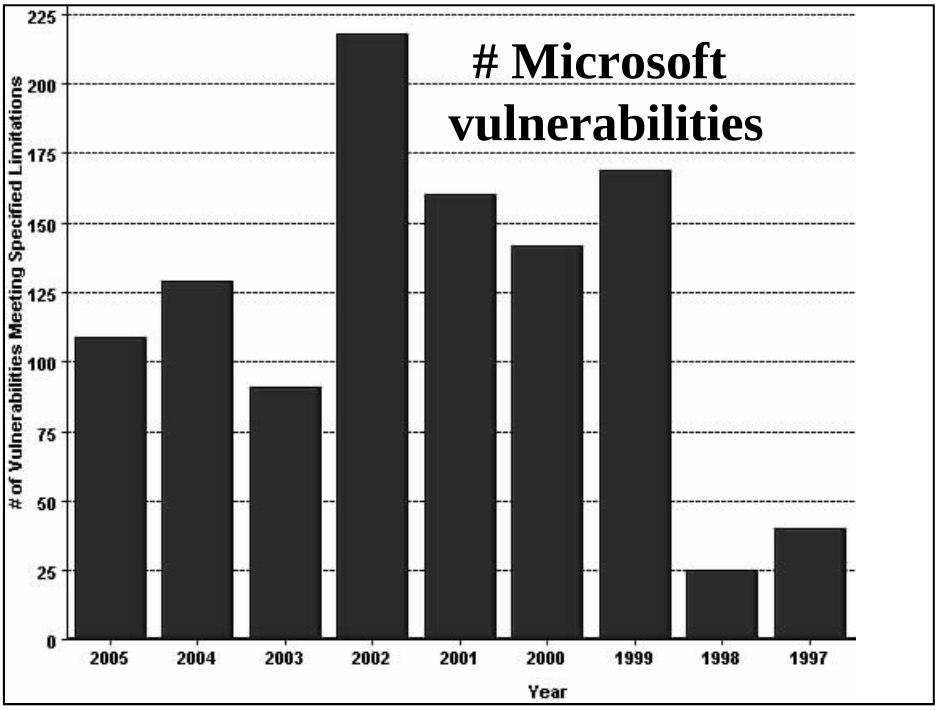


Figure 8

On the graph of vulnerabilities for Microsoft products, the last three years show the fruits of their security initiative to reduce vulnerabilities in their products (Figure 8). Still, the company's products are maintaining at around one hundred vulnerabilities per year.

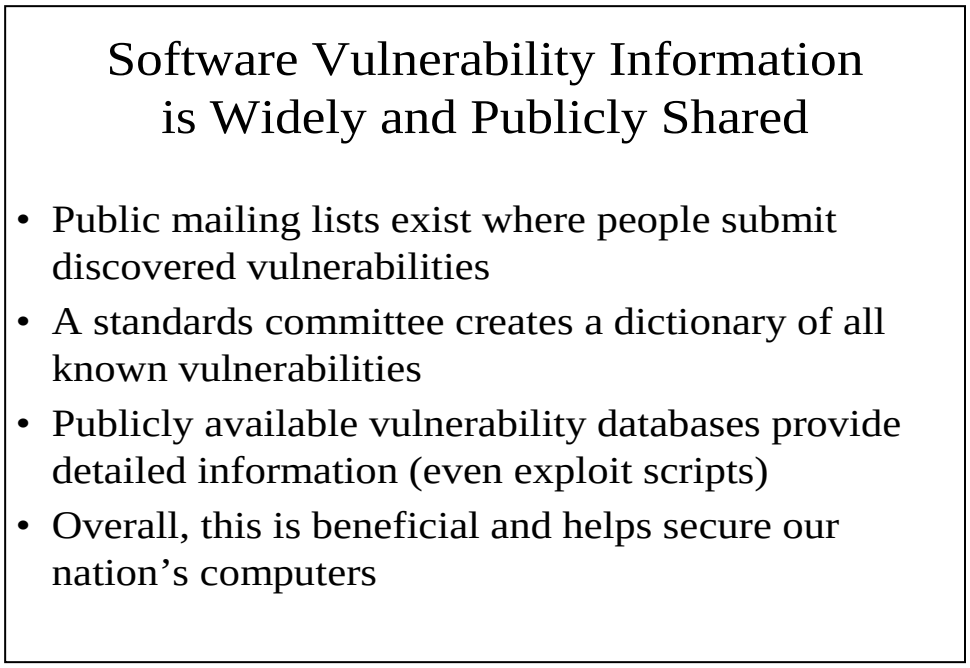


Figure 9

People in the computer industry debate when and what extent to disclose information on security vulnerabilities. However, the industry universally accepts the value of publicly disclosing the vulnerabilities as a way to improve the nation's computer security (Figure 9). Everyone benefits from public audits ensuring that vulnerability has been fixed.

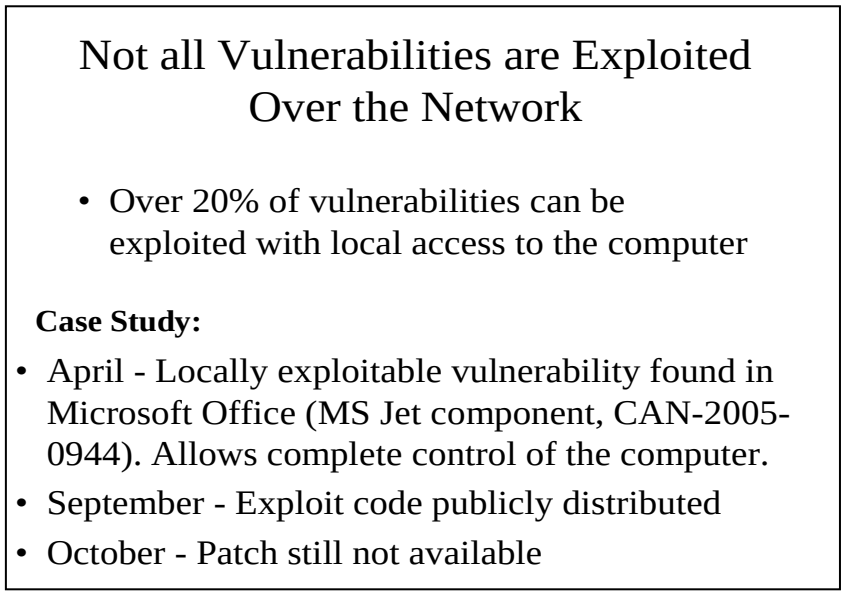


Figure 10

Not all hacking is done over the Internet. Approximately 20% of security vulnerabilities occur locally on a computer (Figure 10). A case study in April 2005 revealed a local vulnerability that affected Microsoft Access and allowed complete control of the computer. As of October 2005, a patch for the vulnerability is still not available. (Vendors are not always able to release patches quickly.) Some voting systems utilize Microsoft Access.

During the question and answer session, Mr. Mell noted that categorization schemes for types of security vulnerabilities are not useful at this time. They tend to be either too large or not precise enough to input into a software scanner.

Threat Taxonomy Overview

Douglas Jones
University of Iowa

- **Voting Technology in its Administrative Context**
- **The Anatomy of an Attack**
- **A Process View of System Evaluation**
- **The Role of Threat Catalogs**
- **Taxonomy**
- **A Proposed Taxonomy**
- **If We Do This Right …**
- **A Threat Catalog is not a Threat**

the author wishes to acknowledge partial support from NSF grant CNS-052431

Doug Jones, University of Iowa, Department of Computer Science

In his presentation, Dr. Jones discussed valid reasons for creating a threat taxonomy, why we need it, and how we would use it.

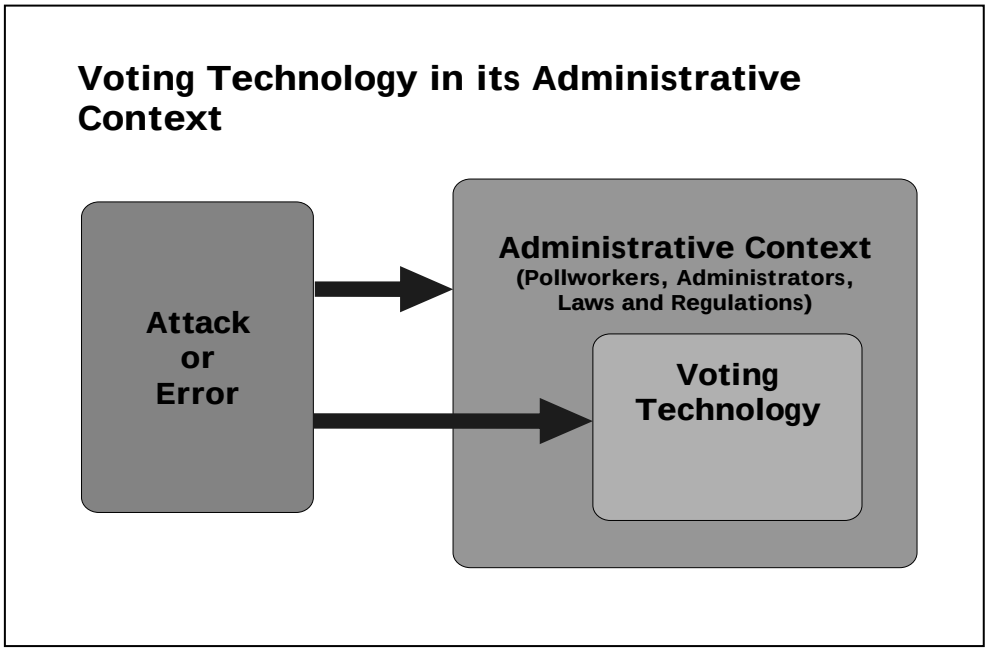


Figure 11

Within the context of a threat analysis, election officials will point out that it is not just the technology, but also the administrative procedures that play an important role (Figure 11). The three "p's" of elections are people, policies, and procedures. An understanding of the administrative context is crucial to analyzing threats of attacks. There is a tendency in the software world to look at the software components in isolation. Dr. Jones pointed out the need to enlarge the voting system perspective to look at the threats for attacks or errors within an administrative context. Attacks can occur inadvertently.

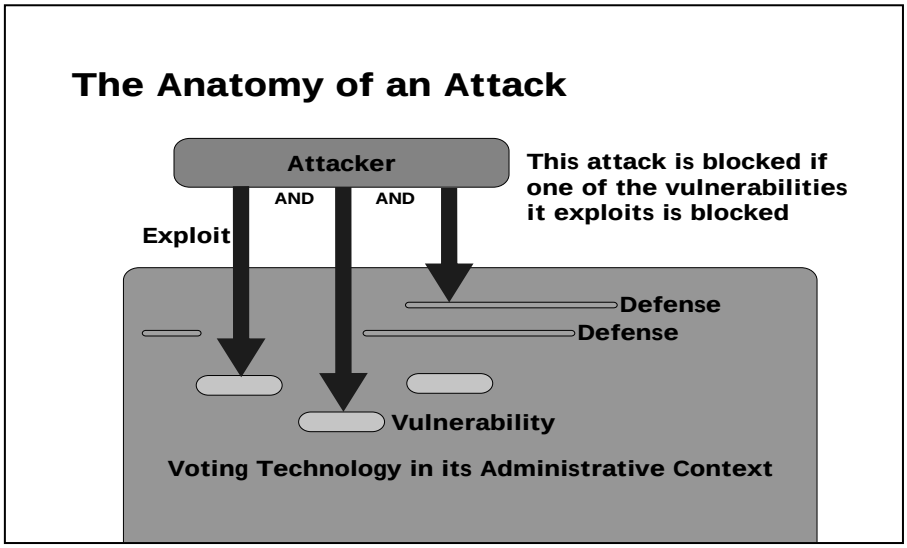


Figure 12

Before discussing taxonomy, Dr. Jones discussed the need to agree on relevant terminology. Someone attacking a voting system needs to identify a set of vulnerabilities. An attacker usually exploits a subset of the existing vulnerabilities of a system (Figure 12). The vulnerabilities are often procedural and technological.

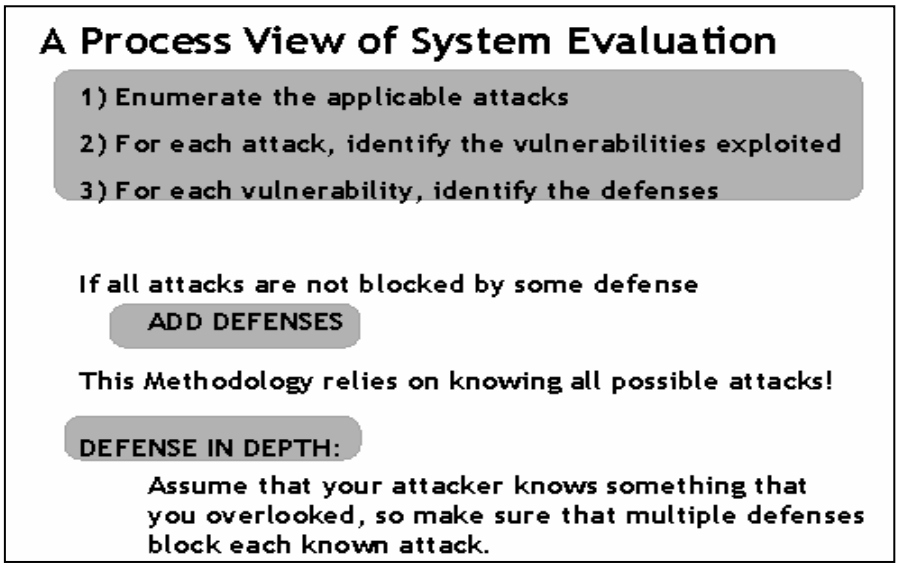


Figure 13

Designing defenses against particular hypothetical attacks does not always work. Frequently, the attacker will exploit a vulnerability against which the system has no protection. In the case of the anthrax attack against the U.S. Senate, the payroll office was protected because of defenses it had created to Y2K vulnerabilities- completely unrelated to the Anthrax attack. Figure 13 describes two methodologies: first, a standard planning process that assumes you know all attacks. A second methodology assumes you will overlook attack possibilities. So you create multiple defenses. This defense in depth methodology provides the system with the potential capability to defend against an unforeseen attack.

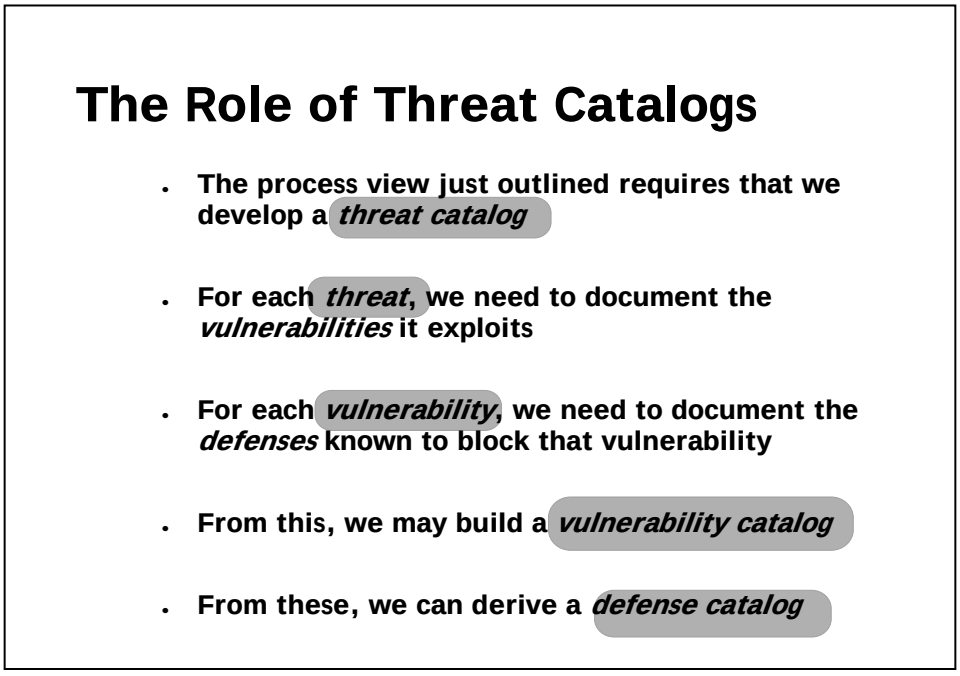


Figure 14

A defense in depth process requires the creation of a threat catalog: a collection of all the attacks on a system thought possible. In addition, documentation of vulnerabilities and defenses for each threat allows a planner to build vulnerability and defense catalogs.

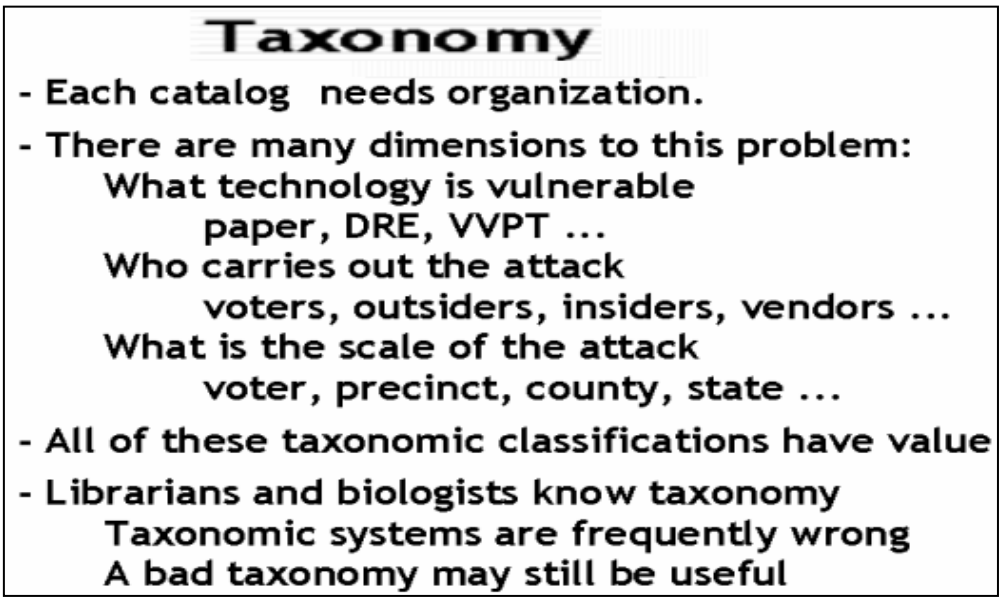


Figure 15

Threat catalogs need organizational structure to be useful. In areas such as biology and library science, taxonomic classifications work well as an organizational tool. Figure 15 offers three possible dimensions for threat catalog taxonomies. Each has potential value. Librarians and biologists are acutely aware that first drafts of taxonomies are often inaccurate. They can still offer useful guidance towards the development of an improved taxonomy.

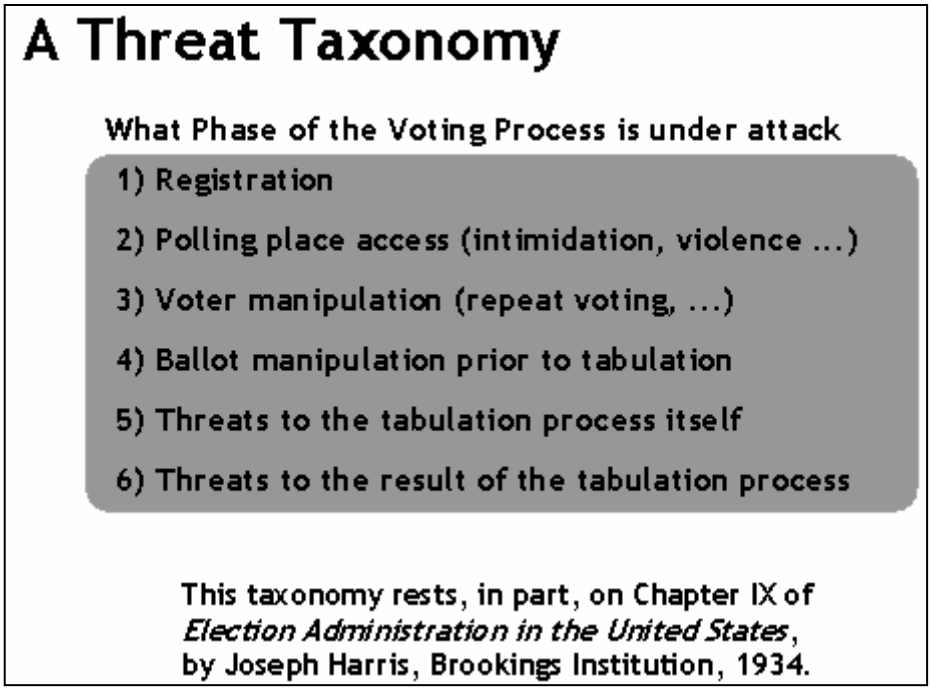


Figure 16

Based on the work of Joseph Harris in 1934, Dr. Jones offered a threat taxonomy classification scheme based on the phase of the voting process under attack in Figure 16. There are both procedural and technological attacks possible in all six phases.

Figure 17

A threat classification based on a well-constructed taxonomy allows you to evaluate both voting system standards and best-practices documents. Figure 17 shows five areas where a taxonomy-based threat catalog will allow you to base evaluations on facts and not assumptions.

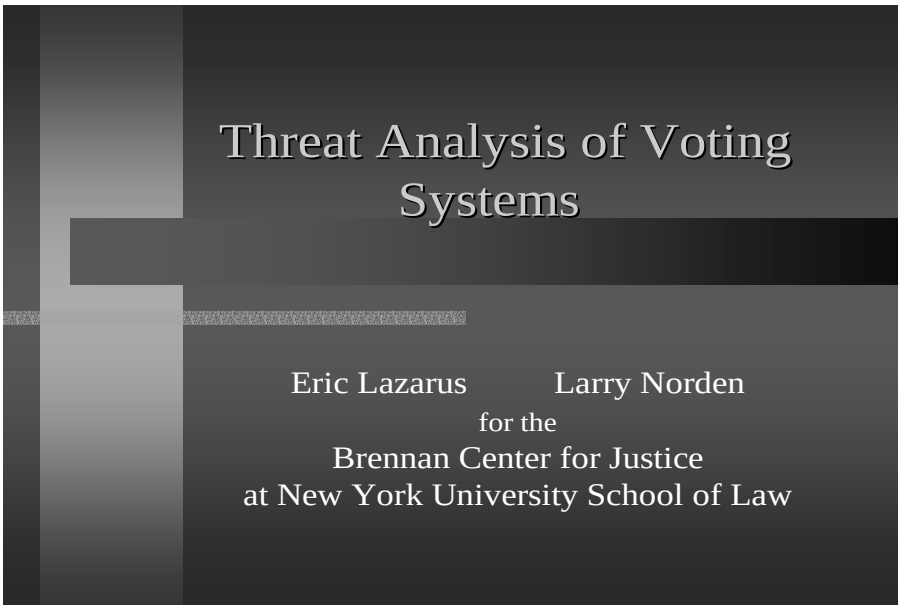
Figure 18

In 1934, Joseph Harris recognized the utility of a voting threat catalog. In the 1800s in a book on lock picking, Tomlinson discussed the value of spreading knowledge concerning election rigging mechanisms (Figure 18).

During the question and answer period, Dr. Jones reiterated the value of starting what may turn out to be a “bad taxonomy” simply to motivate the collection of threats. With the addition of examples over time, the taxonomy could be fixed incrementally by a representative small group of editors.

Referring to the lack of a voting threat analysis since the work of Joseph Harris in 1934, he noted that the catalog process needed to be institutionalized. In a contemporary catalog, we need to better understand the interaction of humans and voting technology. The election process is harder to manage than other computer security problems due to the human- technology interface.

Narrative threat descriptions will only be useful in a threat analysis after they are systematically classified into a formal taxonomy that forms the basis of a computer database.



Larry Norden indicated that the Brennan Center has spent the last several months cataloging close to one hundred potential attacks to voting systems. Making the threat catalog useful to the election community, especially decision and policy makers, has been challenging. It is useful to review the limitations of a threat catalog. Accuracy of voting systems, usability of voting systems and cost of voting systems are as important as security of a voting system. In their review, the Brennan Center did not examine technology-neutral threats to voting systems such as voter intimidation or voter roll manipulation.

The Brennan Center has concentrated on security threats to and counter-measures for voting systems themselves, especially vulnerabilities that will affect a large number of votes and thus the outcome of an election.

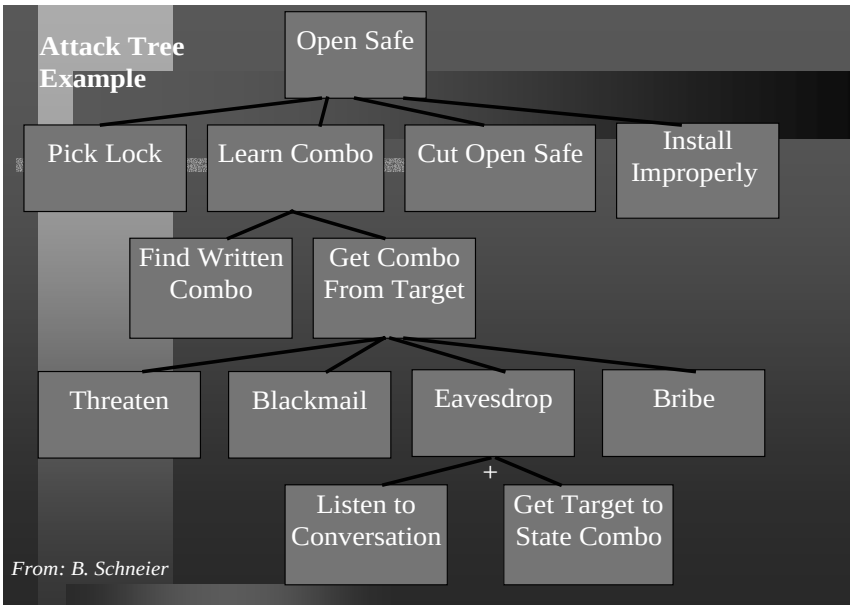


Figure 19

How seriously do you take each potential threat on a voting system? How do you balance priorities on both security threats and countermeasures? To examine these questions more fully, Eric Lazarus defined a threat tree approach not only as shorthand for organizing a collection of potential attacks but also as a repeatable and objective approach to analysis of threats to voting systems. Figures 19, 20, and 21 illustrate an example of an attack tree for opening a safe. On the first row, the tree structure defines the possible choices for opening the safe (the high-level goal). The example follows down methods to learn the combination, then methods to get the combination from the target, and finally the two required methods for eavesdropping to be successful.

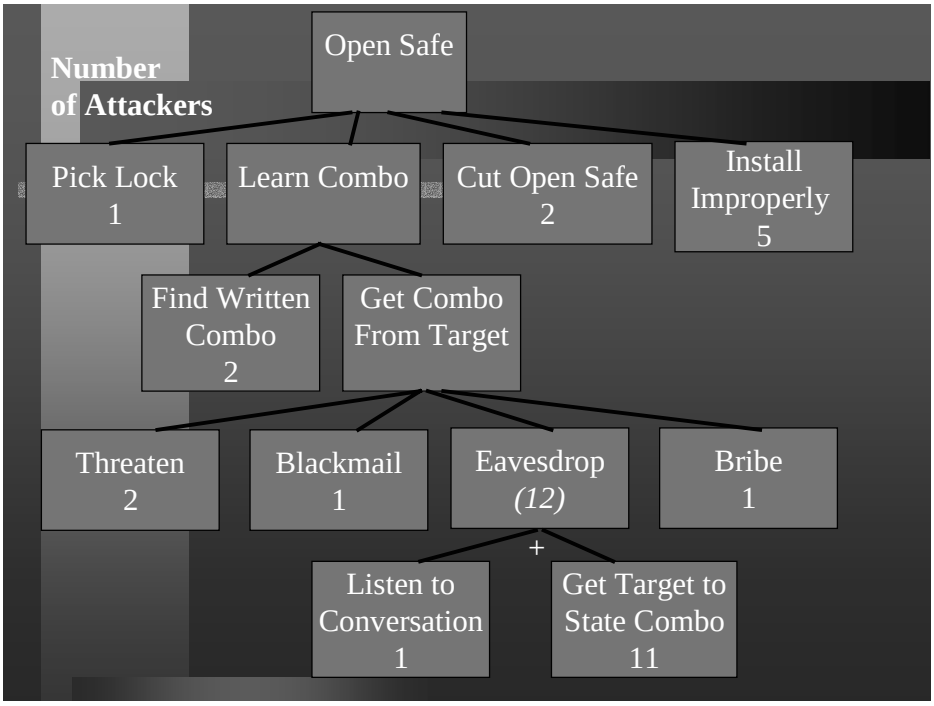


Figure 20

Figure 20 annotates attack plan steps in the tree with degree of difficulty information. In the illustrative example, the boxes contain the number of attackers hypothetically required to accomplish each task. The fewer the number of attackers required, the less the degree of difficulty. In the case of voting system attacks, we should be concerned about high-impact attacks: ones that can steal sufficient numbers of votes to overturn the outcome of a close election without being too difficult (i.e., too detectable for the attacker).

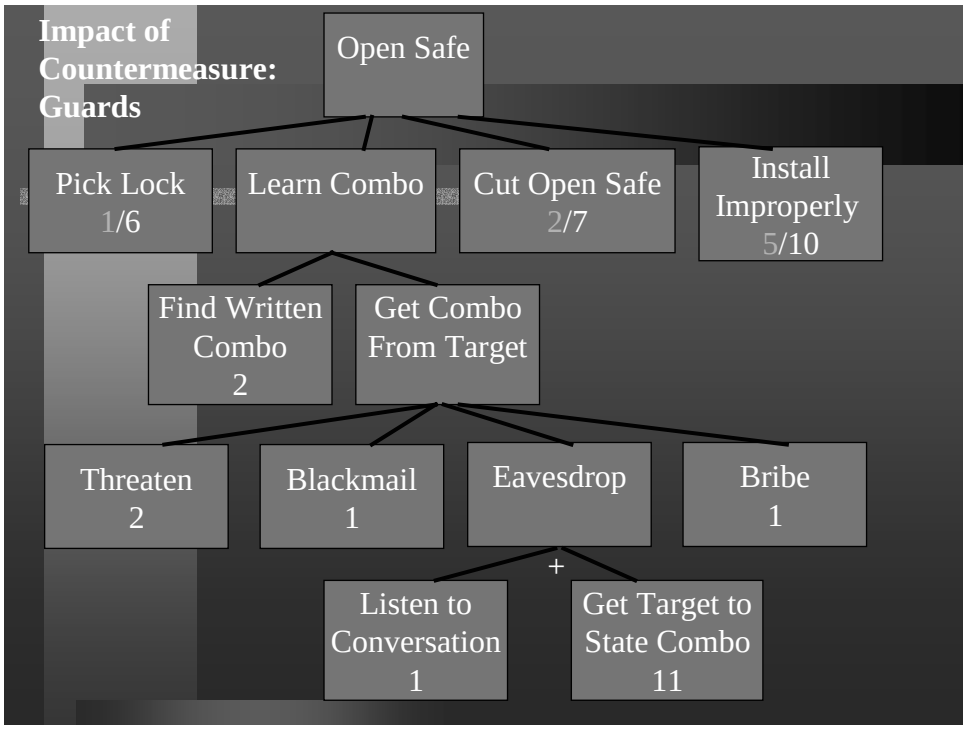


Figure 21

Figure 21 illustrates the potential value of countermeasures on safe attacks. Assume that this business puts guards out front of the building housing the safe. For the plans that require breaking in at night (assume that those are: Pick Lock, Cut Open Safe, or Install Improperly) the teams require five people with guns so each of these plans now go up in difficulty, as measured by likely team size. The value of a countermeasure is quantified in terms of the difficulty of the plan for the attackers. The key is to determine which countermeasures will make the easiest attacks on a particular technology the most difficult for attackers.

Summarizing how to use the threat tree model with a voting system, Mr. Lazarus pointed out that you first need to determine a model jurisdiction for potential attack. This determination provides data such as number of poll workers and voters for building the threat tree. The modelers then need to agree on a level of attack difficulty. This data is annotated on the attack tree steps along with the impacts of countermeasure data. The modelers can then examine the effects of adding or removing specific countermeasures that increase the difficulty of a high-value attack.

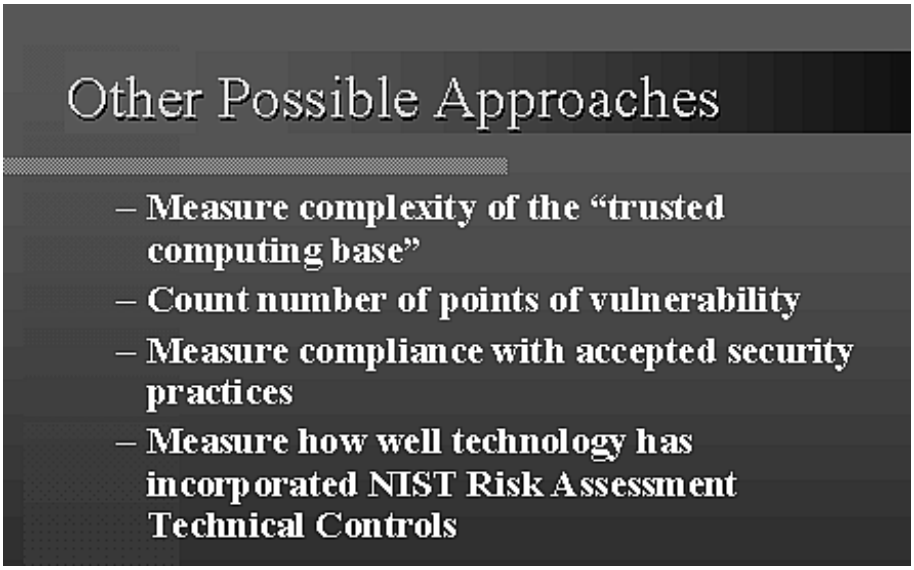


Figure 22

The Brennan Center looked at other approaches to threat classification (Figure 22). Measuring complexity of computer programs (lines of code) can lead to the erroneous conclusion that voting systems with less technology are more invulnerable to attacks. Counting the points of vulnerability in a system can also lead to a similar erroneous conclusion regarding security. Voting has unique security issues. Thus measuring a voting system's compliance with accepted security practices in other venues does not address many of the vulnerabilities that are unique to voting systems.

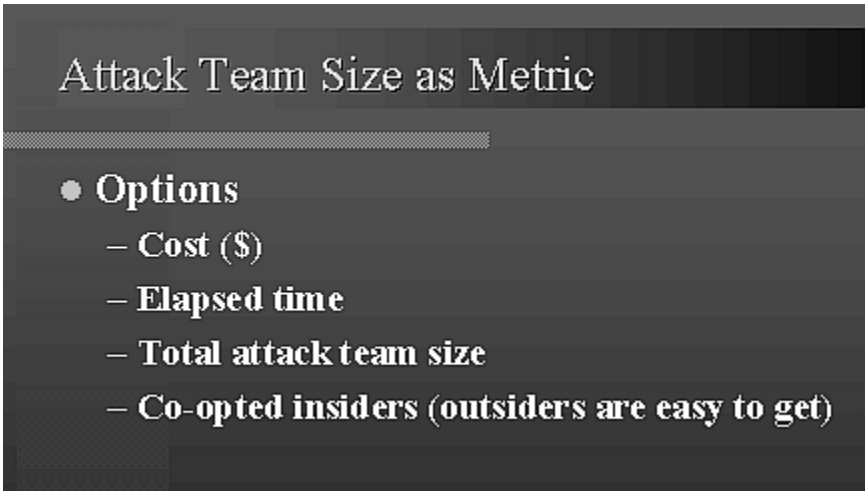


Figure 23

Applying the attack tree to the voting security problem also requires that you initially examine costs involved for the attackers, attack team size (difficulty), and elapsed time necessary for an attack to take place (Figure 23). Cost is a relative measure and is not useful as a way of distinguishing the attacks from one another.

It may be rational to use time to measure strength of a safe. For the strength of election systems, it is not so relevant. When would you even start the clock? While it is clear why the attacker must act swiftly in a bank robbery; it is not clear why speed is important to the attacker in the case of election fraud. It is plausible to examine whether an insider can attack from within an election office (co-opted insiders).

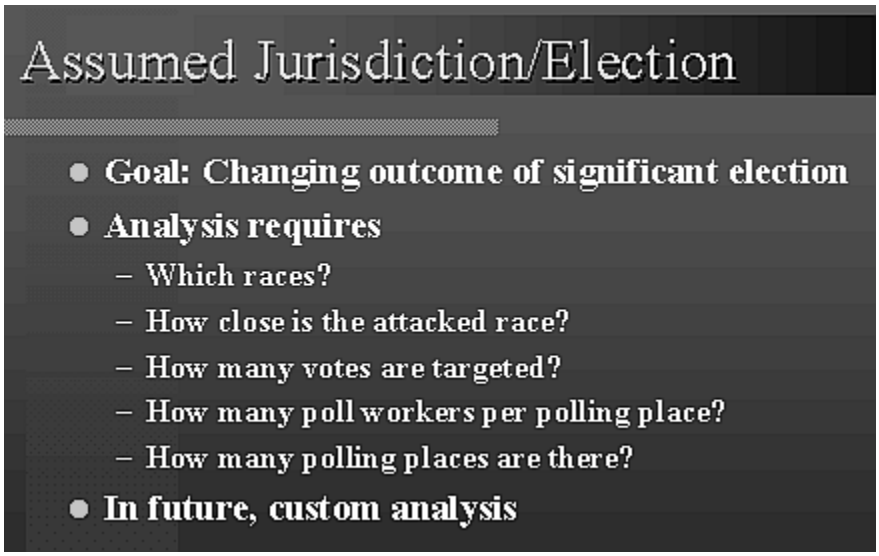


Figure 24

Mr. Lazarus noted that the Brennan Center wanted to find jurisdictions that are typical of the elections we most need to protect (Figure 24). Having secure election systems that give us confidence even when the election is "freakishly" close may not be practical yet. On the other hand, it does not make sense to focus too much attention on attempted fraud against elections in which the outcome is a foregone conclusion. In the end, we may want to perform an analysis of attack difficulty based on the most plausible assumptions. For example, picking a highly populated county for analysis would make sense since an attacker could steal enough votes in that single location to influence the outcome.

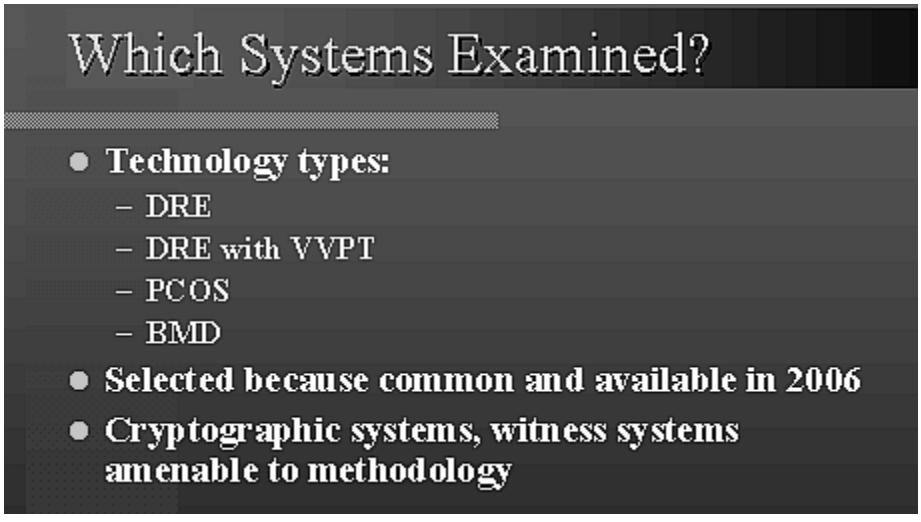


Figure 25

The Brennan Center's attack tree analysis will focus on four types of voting systems (Figure 25). Those systems are Direct Recording Electronic (touch screen) Systems with and without paper printers; precinct count optical scan systems, and ballot marking devices. This same sort of analysis could be applied to cryptographic and witness voting systems.

Panel 1- ***Threat Discussion on Trojan Horses, Backdoors, and Other Voting System Software-Related Problems***

Paul Craft, Douglas Jones, John Kelsey, Ronald Rivest, Michael Shamos, Dan Tokaji, Dan Wallach

Moderator: Barbara Guttman, NIST Information Technology Laboratory

The panelists introduced themselves.

John Kelsey, NIST Information Technology Laboratory, Computer Security Division
Michael Shamos, Carnegie Mellon University
Dan Wallach, Rice University
Dan Tokaji, Ohio State University, Moritz College of Law
Ron Rivest, Massachusetts Institute of Technology
Doug Jones, University of Iowa
Paul Craft, Voting Systems Certification, State of Florida

Guttman introduced the threats to be discussed by the panel (Figures 26, 27) and the questions to be answered (Figure 28).

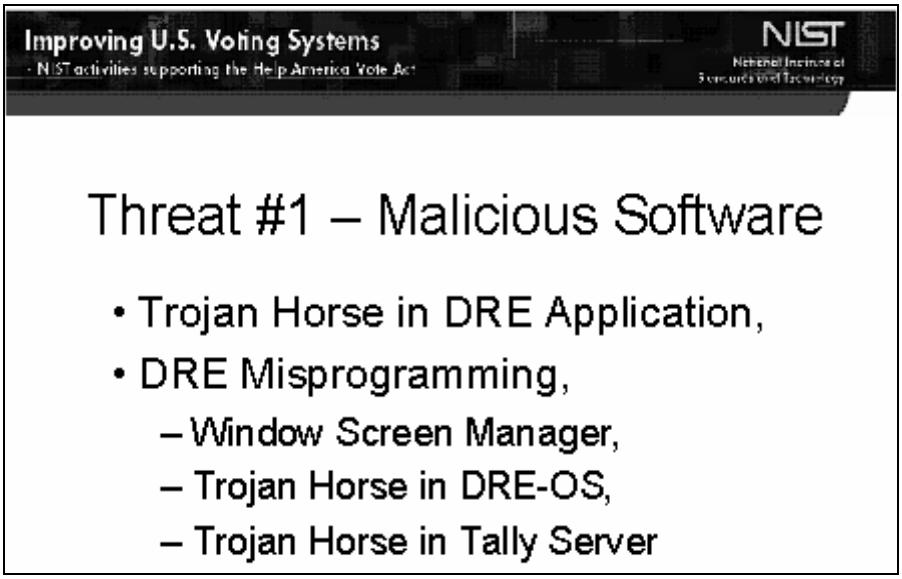


Figure 26

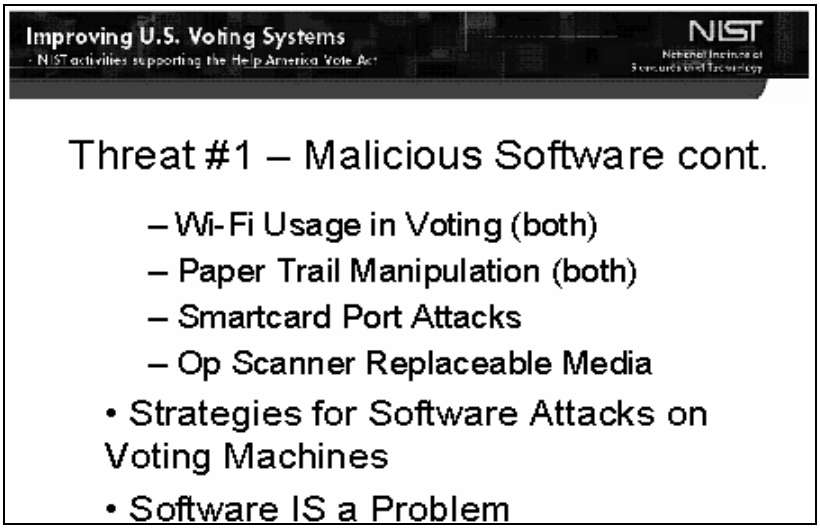


Figure 27

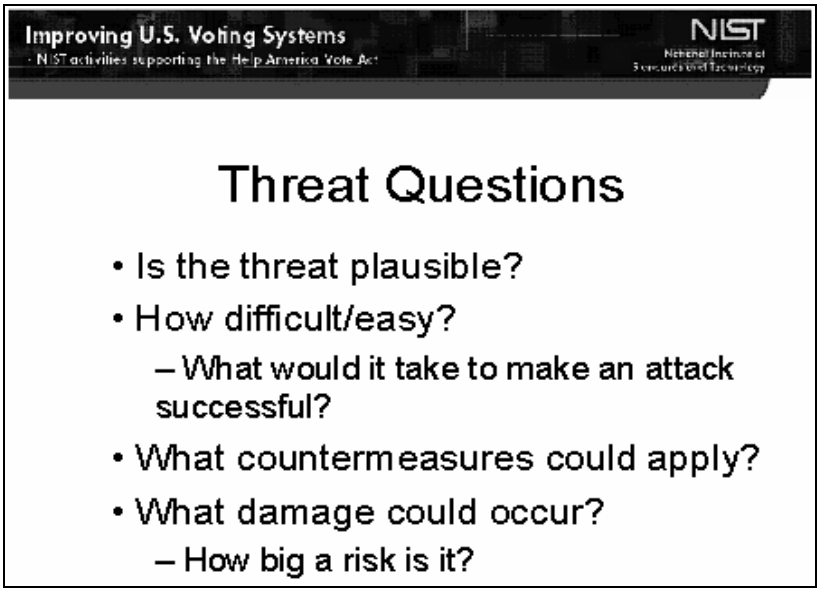


Figure 28

Discussion of malicious software threats:

Craft indicated he thought the threat was plausible, especially with software where the point of origin cannot be determined. There are probably jurisdictions in the United States where you cannot account for the origin and whether the installed version is the certified software.

Jones noted that in Iowa, California, and other states, uncertified software has been discovered by officials. The problem goes a level deeper. There is no way to determine whether a closed voting system is running the version of the software that it displays on self-check.
Jones described a non-malicious attack in Iowa that resulted in the introduction of an unintended "Trojan horse" bug by installing a Microsoft Windows 95 operating system maintenance software upgrade that was not certified.
Craft noted that, in one instance, the threat can be alleviated by validating the firmware for DRE equipment before installing it on the machine. It requires that the election administrator maintain

strict custody of the DREs after loading the validated software. Still, we need better ways to validate firmware after installation. We also need to develop firmware/software system validation into a simple process for all election officials.

Rivest agreed that malicious software is a real threat. Certification of software is indeed a sanity check and provides a level of assurance. But the process by itself will not find all of the bugs and malicious Trojans inside software. Probably most of the bugs inside complex voting software are non-malicious. The software code development process offers another approach to increase quality assurance. A third controversial approach is the use of open source code. Set-up validation is critical to the process in the ways mentioned by Craft and Jones previously.

Tokaji highlighted pre-election, election, and post-election countermeasures as safeguards including certification and parallel testing.

Craft noted that instances of "prior art" countermeasures often are overlooked. State and federal election codes evolved as mitigations to threats that occurred in previous elections.

Wallace addressed his initial remarks to the size of the trusted computing base: the things that have to work to make sure the system is secure. You need to minimize the places where an attacker can attack the system. Smart cards are a potential entry point for an attacker. Substituted malicious cards have the computing capability to reprogram a voting system. You can mitigate the threat through strict procedures or simpler designs of voting systems.

Shamos remarked that it will be important to prioritize the threats by levels of risks and potential gains from addressing them. He also brought up the features of voting software that the voting system vendor discloses to the customer but not to the examiner. An example is a feature that allows election officials to change the election total after the election "if needed." Examiners find software bugs of which the vendor was aware, and examiners also find bugs unknown to the vendor. We need to be concerned about software as distributed separate from malicious attack.

There are no mechanisms for source code control or object code distribution effectively in place anywhere. Georgia has the best mechanism where the vendor sends the software to Kennesaw State University where it is vetted before it is sent to the jurisdictions. This moves the locus of trust from the vendor to Kennesaw State. A single locus of trust can still be an issue.

Shamos indicated that his key software tampering issue is whether an election can be conducted and an intrusion not detected. From his viewpoint, an unrealistic scenario is one that assumes a hacker can change an election outcome in a way that no manner of pre-election, election, or post-election testing or code reading can reveal the intrusion. There are numerous realistic intrusion scenarios, and an outcome for the workshop could be the enumeration of effective countermeasures.

Kelsey pointed out that examiners will not catch all the bugs in a program even in a thorough review.

Craft agreed and noted that one policy in place is to review software after each election to find new bugs. Software testing is in fact sampling methodology and will never be perfect.

Kelsey commented on Shamos' unrealistic attack scenario description. The point here for Kelsey is whether the attack would be caught with the procedures currently in place. While it is likely that software attacks can be successful, it is also likely that the attack can be detected.

Craft noted the need for more research into the plausibility of the attack threats. Individuals theorizing some of the threats are not aware of the scale of effort required to conduct the intrusion. To intentionally change firmware requires numerous individuals and levels of effort that are beyond the capability of a single clandestine hacker.

Wallach noted that it is much easier to attack a latent flaw in the software than to craft a malicious variant of the software. He challenged Shamos' scenario in that it does not address the complexity of the problem. He posited that a sufficiently crafty adversary could hack into voting software and go unnoticed, as did Ken Thompson's hack of C code (see http://www.acm.org/classics/sep95/).

Shamos noted that proving or disproving the existence of the "omniscient hacker" is impossible. He then initiated a discussion of parallel testing. His recommendation to the Secretary of State of California involved empowering a team of people who could walk into any precinct on Election Day and pick any DRE which is then cordoned off from the other machines. Throughout the day, a stream of people operates the machines as if they were voters. However, in advance, the team's examiners know the outcome of the votes for that machine. The voting is videotaped to capture voter errors. At the end of the day when the polls are closed, the parallel testing machine is also closed, and the vote total is compared with the expected total. Similar parallel testing teams operate throughout the state. In theory, any organized attempt to influence the election would be captured if enough random precincts are targeted. The question for the panel is whether the testing effort is worth the cost as a countermeasure.

Craft was not sure that parallel testing was an effective countermeasure. However, it mitigates many of the conspiracy theories. The best defense against bad software code is controlling your system and managing procedures. Parallel testing provides an understandable proof and level of assurance that correct procedures have been implemented.

Shamos and Craft agreed that parallel testing was an effective attack detection measure.

Rivest indicated that parallel testing put up a steep fence for an adversary to scale. However, he raised the possibility of an adversary determining in advance which machine was to be used in parallel testing through a signal by a voter to the DRE. Also, while parallel testing adds value, it also adds expense.

Shamos indicated that you would need a fairly large conspiracy to carry out the signaling exploit for every voting machine. Local elections are most vulnerable to the signaling type of attack, especially in elections where every ballot is different in every precinct. Countermeasures need to be explored here.

Rivest raised a concern with wireless technology as an attack method to signal to multiple voting machines all at once. Shamos agreed and stated that wireless technology and voting do not mix.

Kelsey and Jones began a discussion of state recount laws and their applicability to unexplained and unexpected (surprise) election results. Tokaji recommended a review of state election recount laws available in his paper, *The Paperless Chase: Electronic Voting and Democratic Values*, September 2004 (see http://www.dos.state.pa.us/election_reform/lib/election_reform/Paperless_Chase.pdf).

Jones indicated his concern with an accepted definition of firmware as precedent by the Independent Testing Authorities (ITAs) for voting systems. The ITA-accepted definition of firmware is software that runs on the voting machine in the precinct. So software resident on a PCMCIA card was defined as firmware.

Panel 1 Audience Participation:

Question/Comment: Tencati addressed a question to Rivest and Kelsey: With the common criteria, digital signature capability, and FIPS 140 standards, are not some of these malicious threats mitigated? Rivest noted the issue of complexity of software and the voting process. He also noted the need for the proper use of cryptography and key management in the development of voting systems. Kelsey noted that the FIPS 140 standard does not address the insertion of malicious code by the vendor or a COTS software programmer.

Question/Comment: Saltman raised for discussion the reduction of software size so that it is manageable to test. He noted that what is essential is that the system software is correct. The number of bugs that can be found is inversely proportional to the size of the software program. The issue is the correctness of software that could eliminate the possibility of malicious software. Software with millions of lines of code is not required to run individual DREs. Single-function, process control software would seem more appropriate here. Large COTS software operating programs often cannot be tested for bugs.

Rivest agreed with Saltman's premise. He offered one possible solution that divides the voting process into two parts: composing the vote and (security critical) casting of the vote. The user interface in the vote composing section requires the advanced software code. The casting of the vote would be done at a separate secure station with a manageable software program. (See Cal. Tech-MIT Voting Project Report, http://www.vote.caltech.edu/reports/2001report).

Craft noted that simple, concise, and well-formed code is desirable. The voting process with HAVA has become more complex. Today's voting system has to talk in a variety of languages with variable audio and visual features. Provisional voting and early voting along with complex graphics also compound voting system requirements. The biggest problem with system security and software integrity results from changes in user demands over the last five years. Jones referenced the avionics industry as a model, where spending on software testing and certification is ten times the amount spent on software development. In voting systems, relatively small amounts of money are spent on testing versus the amount spent on software development. In the future, what the commercial voting industry needs is small, easily reusable COTS software modules developed to high standards. However, designing unique software for voting systems is financially burdensome. Shamos noted that an electronic election in India was successful for 360 million voters. The voting machines were hardwired and the election itself simple. Ballots are too complicated in the United States to use the Indian system.

Question/Comment: Hall asked the panel to address disclosing source code as well as the commercial pressures on voting system vendors with respect to trade secrets. Shamos noted that there is a difference between open source and disclosed source code. Disclosed source code is critically important. The public needs to be able to verify the integrity of software for themselves. Shamos stated that commercial trade secrets and voting software are inconsistent with one another in this instance, due to the high impact of secure voting on the democratic process. He indicated that there is no competition solely in voting system software. Wallach noted that publicly available voting system software would result in the development of more secure software in the long run.

Question/Comment: Klein raised the issue of differentiation between attacks and equipment malfunctions. The current voting system reliability standard for mean time between failures allows an Election Day failure rate of 10 percent (163 hours MTBF). Some failures are due to unacceptable electrostatic discharge rates. Antistatic procedures are currently insufficient. It is difficult to separate reliability from individual attack threats. Kelsey noted that masking your attack as an error is plausible. However, Shamos proposed that most instances of system unreliability are honestly that. The current MTBF is unacceptable, and it should be upwards of 1000 hours. Craft noted that most voting machines in production attain a high MTBF rate. However, we need to look at ongoing quality assurance issues in future voting system standards. Klein raised the point that in Maryland, there was data to indicate that voting systems did not meet the 163-hour standard. Jones raised the issue of complex policies and procedures for election workers. Failure to plug in voting machines resulted in a "low battery" failure rate of 10 percent in one instance in Florida. The failure was a procedural failure.

Question/Comment: Freeman noted that the 163-hour MTBF was set on central counting systems twenty years ago. The model back then represented five years of use. The use of voting equipment has increased exponentially since then. Looking at threat analyses, closed DRE systems do not allow for an external check for integrity at the point of execution. You need to consider less restrictive countermeasures as a trade-off so that you can perform adequate safeguards against an attack approach. In addition, validating software can result in discovery of unrelated files and programs outside of the context of the voting software.

Question/Comment: Weatherbee noted the use of the common criteria by the defense community to solve the problem of certifying software code. He asked the panel to comment on the possibility of requiring voting system vendors to meet a protection profile for voting machines that could be developed through peer review by the technical community. He also asked the panel to comment on the certification process required for gambling slot machines in Nevada. Shamos agreed that the technology exists to create highly trusted and secure computer systems. However, the funding available to the defense and the gambling industry to create these secure systems far exceeds the funding available to the election community and the voting systems industry. He noted that, at this time, not enough concern for increased security of voting systems has been voiced by the public to elected officials. A heightened awareness could eventually provide the funds to increase security requirements. Jones commented favorably on Nevada's certification of gambling machines as a model to emulate for future voting systems. The system for verifying that the software versions are correct requires additional hardware on each slot machine. The module that does the version control is produced and owned by the state.

Panel 2- ***Threat Discussion on Voting System Configuration Issues and Problems***

Jeremy Creelan, Dana DeBeauvoir, Douglas Jones, Avi Rubin, Ronald Rivest, Ted Selker, Michael Shamos

Moderator: Barbara Guttman, NIST Information Technology Laboratory

The panelists introduced themselves.

Michael Shamos, Carnegie Mellon University
Ron Rivest, Massachusetts Institute of Technology
Doug Jones, University of Iowa
Jeremy Creelan, NYU School of Law
Avi Rubin, Johns Hopkins University
Ted Selker, Massachusetts Institute of Technology
Dana DeBeavoir, Travis County, Texas, Clerk

Rubin first briefly described the NSF-funded ACCURATE project for studying security issues related to electronic voting. The NSF is the principal source of funding for university research into computer security issues. The funding is for basic research, education, and outreach. The purpose of the ACCURATE project is to create a platform of technology which others can use to make future voting systems more secure, accessible, usable, reliable, auditable, and transparent.

Guttman introduced the configuration and calibration attacks for the panel to discuss (Figure 29) and the questions to be addresses (Figure 30).

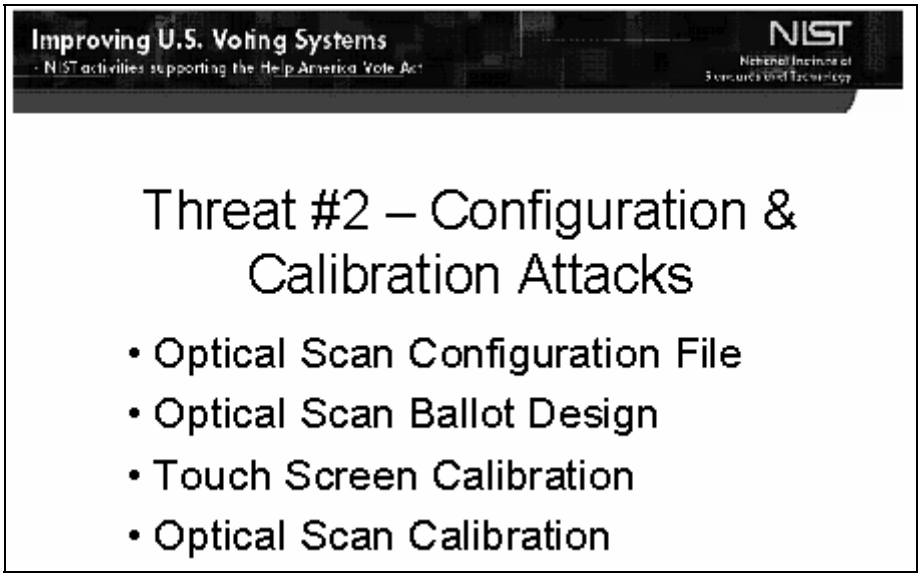


Figure 29

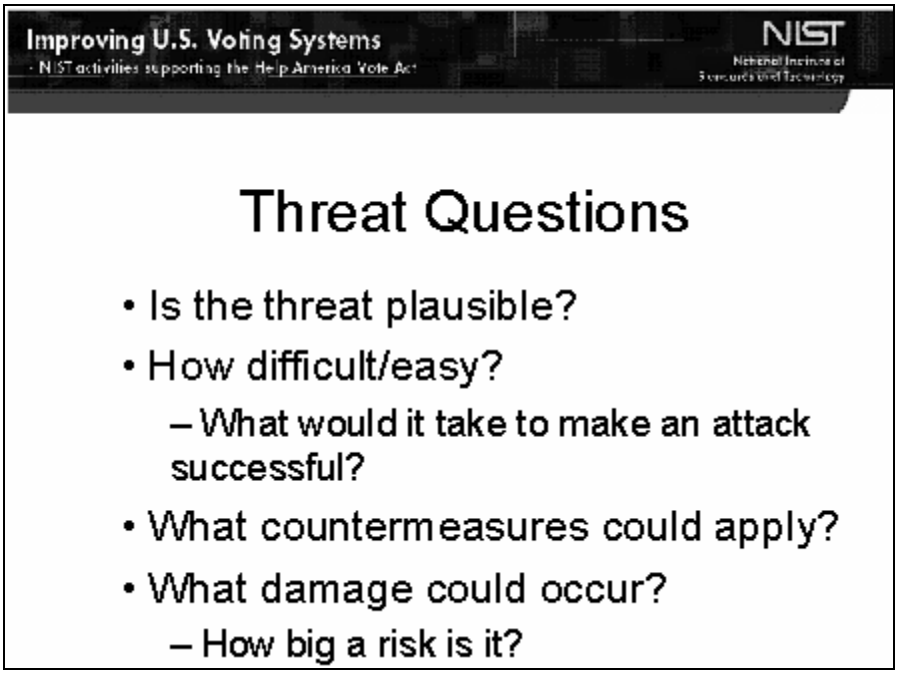


Figure 30

Discussion of configuration and calibration threats to voting systems submitted to the workshop in advance:

Jones noted that the optical scan configuration file attack and the optical scan ballot file attack are two sides of the same coin. In op scan voting systems, there is no direct linkage between the candidate and the counter that is used to count that candidate's votes. The ballot scanner only knows that there was a mark in a certain column and row. Inside the voting system is a configuration file that relates a position on the marked ballot and relates it to the candidate. The crucial configuration files have two sides to them: one configures the voting machine to count votes for candidates and the other is the file of information that goes to the printer to have the candidate's names printed in the correct location. These represent two distinct attacks: one attack against the information going to the printer and the other, an attack on the file that goes to the tabulating machine. In one way, the touch screen calibration problem has similarities to the op scan problem. The touch screen device on a DRE is not the display screen but rather a thin transparent device that sits on top of the display screen. There is no direct connection between the coordinates that are sensed and the coordinates of a particular object on a display screen. Calibration is required. The mapping between the two represents an attack vulnerability. In the past, routine mistakes also have been made in the printing of ballots and in ballot configuration file generation.

Jones pointed out that optical scan calibration is a different issue. Here, it is a question of how dark a mark is required to be counted as a vote. If you have a ballot where calibrations can vary from precinct to precinct, you have the opportunity to make votes more likely to be correctly (or incorrectly) recorded in some locations than in others. The old ES&S central count scanners have separate photo sensor LED pairs looking at each column of the ballot. Those sensors are separately calibrated. Unless the sensors are calibrated correctly, the standard for what counts as a vote could differ by column. Counties do not always check this calibration. The 2002 VSS does

not address the calibration issue because it is a human factors issue. There is a potential countermeasure here with new software from Hursti that would make tif file images of the ballots publicly available as an independent check on the counts.

Shamos noted that voters are intuitively aware of op scan voting technology from standardized testing. The ballot choices can be erased and re-marked, and the voter interface is user-friendly. The voter believes that the machine will view the vote as they recorded and viewed it. However, the op scan recognition technology is relatively unsophisticated and marks are not always picked up as the voter intended. States have different regulations defining the acceptable mark that constitutes a vote on an op scan ballot. In Hawaii, if any portion of the mark covers any portion of the oval, the mark counts as a vote. However, any mark outside the oval does not count as a vote. So circling the oval will not count as a vote. Shamos then addressed the calibration issue as it applies to the printer attack on optical scan voting. There are varying levels of friction in the rubber rollers that pick up the paper ballot in precinct op scan machines. Large black rectangles on the side of the ballot called timing blocks tell the op scan machine where to look for marked ovals. The blocks are made by the printer and tell the machine precisely where to look for the voter's mark. If the printer offsets the timing mark from the ovals, then the area over which the op scan will recognize a vote is reduced. Thus slightly variant marks in the ovals may not count as recognized votes by the scanner.

Craft recognized the attack threats described by Jones and Shamos as real and serious. However, he pointed out that simple mitigation techniques already exist in the form of effective management of the process by election officials. Checking configuration, proofing ballots, as well as testing machine components well before the logic and accuracy tests, will mitigate each of these threats.

Rivest noted that with calibration threats, there is plausible deniability for the attacker. With respect to the scanning attacks, a feedback mechanism would be useful as a mitigation tool. In converting from the analog (paper ballot) to the digital (op scan electrical record of vote), feedback would provide the voter with assurance that the vote was recorded as intended. Such feedback would be in line with the concept of equivalency in independent dual verification.

Selker commented on the critical need for backup of the configuration files as an essential election management technique. Redundancy is a key mitigation tool. With regards to op scan recognition technology, he noted that China employs a more reliable approach where an image of the ballot is recorded.

Craft emphasized the need for concrete guidance from this threat analysis effort for local election officials by the 2006 election. There needs to be a determination for each type of voting system of realistic risks and mitigations that election officials need to take.

Rubin agreed with Craft's call to action. Listing the threats is important because it begins a process of determining mitigation efforts. In a way, the calibration problems can be viewed as similar to the malicious software problems in that you can mitigate both with independent dual verification. If you are concerned that the op scan machine is not counting correctly, you can mitigate with random manual counts and pairing the results. Another op scan ballot marking device is referred to as the "$5000 pencil." Using a touch screen, the voter makes their selections on the ballot and prints it out. The marking machine makes the selections correctly

with the mark locations hard coded into the voting system. The ballot is then run through the op scan counter. If the attacker is in collusion with the op scan equipment manufacturer, the scanner can be set to offset the marks and read them incorrectly.

Craft noted that neither the Automark system described above nor the various voter verifiable paper trail schemes are mitigations to threats. They are new types of voting systems, each of which need to be cataloged for their own lists of potential threats and attacks.

DeBeauvoir addressed the need to identify real threats and the role of officials in the field conducting elections in both identifying risks and establishing mitigations. Election officials believe that threats and mitigations need to be determined on the basis of a formal risk assessment. Many of the current threats have been proposed by people who are unfamiliar with elections and formal risk assessment procedures. Threats need to be analyzed in terms of the specific equipment used, the specific elections being run, and the control procedures in place. Travis County, Texas, has devised an end-to-end process model that identifies the areas of risk. This allows election officials to logically organize and deal with each individual threat. DeBeauvoir proposed that NIST and the TGDC come up with a list of minimum "common place" technical and procedural controls under which election officials can operate. In addition to the controls, hash code testing offers a basic setup validation tool. Additionally, parallel monitoring has become a politically manageable and common sense mitigation tool that the public can understand in terms of addressing potential attacks in a DRE environment. Chain of custody procedures need to be quantified on the basis of rules of criminal evidence. These include audit logs and tracking checklists, knowledge of the person that created the lists, and methods of securing the evidence. All of these procedures have to be determined for individuals unfamiliar with both risk assessment and assuming little or no funding for the efforts.

Rubin emphasized the need to think in terms of defense in depth covered previously by Jones. Identification of threats and mitigation efforts do not work if minimally trained poll workers do not read the procedural manuals. What is the fallback defense in this case?

Jones noted that management controls work only if the managers implement them effectively. Massive lists of threats and procedures will not work. There needs to be simplification for election officials as well. Also no-fault absentee voting and voting by mail require specific threat analyses and mitigation procedures. Finally, the disconnection between state laws and voting mechanisms is important. Op scan markers in the field actually count circles drawn around ovals in violation of Hawaii's state law. The vendor documentation does not provide the acceptable mark criteria. Instead, you need to test for the counting capabilities of the system to see if it conforms to state law. This includes testing with marking devices other than a number-two pencil.

Creelan brought up the legal concept of "burden of proof." When dealing with the plausibility of threats, you are implicitly dealing with assumptions about the burden of proof. Shamos' previous discussion of whether we believe the "omniscient hacker" is relevant here. To rephrase this in a religious analogy, if the person is an atheist with respect to belief in the "omniscient hacker" on one side of the spectrum, the true believer in the plausibility of every attack is on the other side of the spectrum. Creelan takes the position of the agnostic, in the middle. We do not know in many instances whether a specific threat is plausible. The question then is do we err on the side of placing the burden of proof on the true believer or the atheist? Perhaps it makes sense to be

agnostic, but religious at certain moments, protecting against threats when we are not sure whether they are going to happen. In other areas of law and regulation, the concept of technology forcing is very much part of the debate. If you want to get to an objective, such as reducing real threats to elections, you need to do more than assess current technology. There is value in standards that force technology to develop in new ways to address the threats in the long term.

Craft noted that this discussion brought up the point that while these are threat questions we are asking now, all election officials need to ask these questions with every election cycle. As a manager, you have a finite amount of resources with which to address security threats. You have to evaluate the plausibility of threats in your circumstances. You have to assign priorities and make decisions. At the end, you have to take your experience and go back through the threat model again. It is an ongoing process.

Rivest addressed the specific threat to configuration files and the use of hash functions to compute the digital signatures for various pieces of executable code. It is important to understand that you have different classes of objects that are not fixed and static but change with each election. The objects come from the national, state, and local levels. If you want to authenticate those components of the configuration files, you will need digital signatures on each of those objects which will check them dynamically with each election.

In summary, Guttman noted consensus that the threats discussed by this panel are plausible. She noted that there appeared to be agreement that the attacker would need to have some technical knowledge. Craft noted it would take technical knowledge to keep these threats from occurring. Guttman noted the panel agreed that countermeasures would be classified as managerial but if the procedures are too onerous, they would not be carried out. Craft noted that the countermeasures need to be as simple as possible. Damage that would occur if the attack was successful could include electing the wrong person.

Guttman then asked the panel to discuss the next group of usability threats (Figure 31) and address the requisite questions (Figure 32).

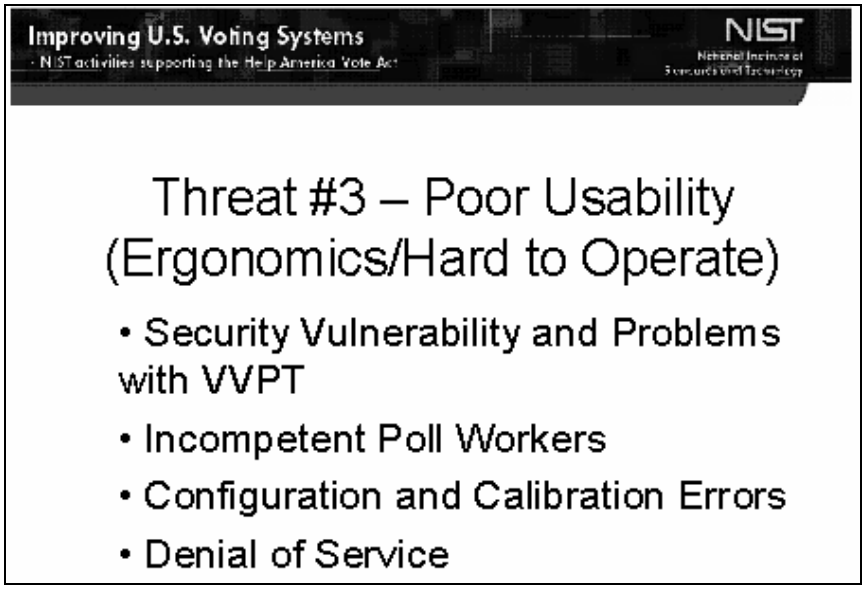


Figure 31

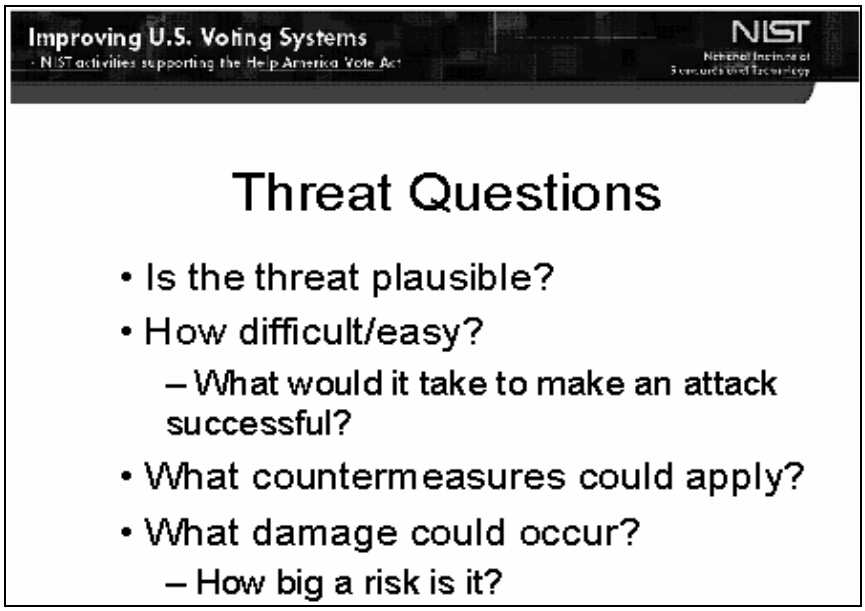


Figure 32

Selker noted that the most plausible instances of hacking exist when people individually have access to the systems. Registration is an example where people put hurdles in front of the voter. Public sources of voter information can result in attacks on Internet sites that provide incorrect information to the voter. Jurisdictions need to take precautions with printed material in much the same way that workers at the U.S. mint handle money. Transmission of election data at the end of the day requires strict procedures. Too many election procedures are carried out by a single person.

Selker went on to state that you need multiple non-colluding "hands and eyes" to prevent and to detect attacks. In the voting process, proper setup of materials for election officials is critical to an effective process where someone checks another person's work. We also need to work on cryptographic solutions that make for simpler voter usability. Audio verification is an example where this second record is used as a redundant perceptual feedback at the time the voter makes a decision. By making the voting process simpler, you increase accuracy.

DeBeauvoir emphasized that you cannot confine security to just the voting system itself. Election administrators must consider the whole election process. You cannot separate out just the voting equipment and hold a secure election.

Shamos highlighted the difficulties of confusing user interfaces with DRE voting systems. These systems vary tremendously in their ease of use. He illustrated the difficulty with the concept of the unexplained undervote. The theoretical minimum estimate for undervoting is .5 percent. This means that approximately one voter in two hundred is unable to cast a vote when they enter the voting booth. An undervote of 2.5 percent means that 2 percent of the undervote is unexplained. Some attribute the 2 percent to deliberate malicious manipulation of the voting machine. Others attribute the unexplained undervote to machine error. Shamos suggested that inadequate user interface in combination with machine error is the source of the unexplained undervote. Inadequate user interfaces result in the voter leaving the voting booth believing they voted one

way, but because of the interface, the machine did not record the vote that way. As an example, in a multi-page ballot, a voter who makes and then cancels a straight party vote will not know the effect on the unseen pages unless they verify each page.

Rubin noted that poor user interface can result in a loss of privacy when the voter has to ask a poll worker for assistance.

Jones referred to the incompetent poll worker attack (see: http://vote.nist.gov/threats/papers/incompetent_pollworkers.pdf). Spoiled ballot processing always involves poll workers. The likelihood of a voter being offered the chance to spoil their ballot and the subsequent likelihood of the process being carried out properly is dependent on the competency of the poll worker. Jones characterized poll workers as a weak link in the security chain. He noted that they are hard to recruit and retain from election to election. Deliberately tampering with the poll worker pool by assigning competent poll workers to precincts that are demographically likely to support a particular candidate and incompetent ones to precincts where voters are not likely to vote for that candidate becomes a plausible attack. Given the competency level of many poll workers, this attack would be difficult to distinguish from an accidental event.

Craft took exception to the characterization of poll workers as a weak link in the chain. They may be a point of risk to which election administrators need to give attention. However, the voting process is extremely complex and depends on many dedicated volunteers. The main reason for the success of the process as a whole is the importance volunteers give to their public service.

Jones replied that he may have incorrectly stated the issue and that he had respect for the people who volunteer unselfishly as poll workers. However, handing a two-inch binder of hard-to-follow procedures to poll workers “borders on the inhumane,” and you cannot expect them to read it.

Rubin asked Craft if thought that poll workers were one of the least deterministic aspects of the election process. Craft agreed that they are an area of very high risk. They are an area that deserves a tremendous amount of election management’s attention. To simply hand them a two-inch binder without sufficient training is negligent management.

DeBeauvoir stated that in many jurisdictions, poll workers are recognized as a group for their bipartisanship and independence in that they watch over each other. Today, poll worker training is not given the minimalist approach of the past. In fact, they become mitigators for threats to the process.

Craft noted that the recruiting and training issue comes back to effective election management. There are election administrators that require poll workers to pass tests before they are allowed to participate in the process. Election administrators that do not follow this procedure due to a lack of poll workers need to go to their county administrators to obtain funding to hire more competent poll workers.

Selker described a spectrum of poll worker training experiences. Poll workers trained conceptually in Chicago with complex materials tended to become confused and make mistakes

on Election Day. Poll workers trained procedurally in California with well-crafted and easy-to-use manuals appeared to carry out their assigned tasks effectively.

Shamos offered perspective on the number of poll workers in the United States, 1.4 million, which is larger than the size of the U.S. Army. There are estimates that two million poll workers are needed to provide adequate support on Election Day. Ten levels of officer grades manage the Army out of the world's largest office building. It is unrealistic to think that the funding exists for a similar management structure to effectively train and manage poll workers to operate at a high level of efficiency. However, the current deficiencies of poll workers are probably due to inadequate election management.

In defense of Jones, Rubin indicated that of the three areas susceptible to security vulnerabilities- procedures, equipment, and poll workers- it is the poll workers that are possibly the least predictable.

Craft reemphasized that poll workers are often the mitigation against many security attacks. For example, competent and well-trained poll workers will handle denial of service strategies efficiently.

Selker indicated that activist poll watchers can intimidate poll workers and represent a security problem as well.

Shamos mentioned that poll workers will be faced with supervising the use of new voting equipment as a result of HAVA. A poll worker checklist of tricks that people may try to subvert the election with the new equipment would be useful.

Panel 2 Audience participation:

*Question/Comment:*Epstein referenced the IT industry's reaction to the Morris worm as the first large-scale attack against what became the Internet. The industry changed how it checked products for security in the aftermath and constantly became aware of and reacted to new types of security attacks. How does the panel propose to do retrospective testing of voting equipment that becomes certified for threats established today?

Shamos described the procedure in Pennsylvania. For a fee of $450, any ten voters can compel the commonwealth to reexamine any voting system in use should a new threat appear. Systems have been decertified in the past when determined to be unsafe.

Craft agreed that the threat review is a constant process initiated after every election cycle in preparation for the next.

*Question/Comment:*Browning addressed the poll worker problem from the perspective of an election administrator. The voting process cannot operate without poll workers. It is a people-driven process. Election management problems that came to light in 2000 existed in previous elections. People policies and procedures always have been and always will be the key to a successful election.

Jones added that there can be an overemphasis on management and an under recognition that technology can, in certain instances, help reduce the need for new procedures. He referred to a hardware design of a memory card that would make it impossible to connect it to a modem (to send election results) without removing the memory card.

Browning replied that while we are trying to simplify policies and procedures, the voting process has, over time, become increasingly more complex.

*Question/Comment:*Fisher asked the panel to address the issue of the insider threat with respect to chain of custody. Does it make sense to have a national certification and accreditation process for election administration at the state and local level? Also, is there a threat with absentee voting or with voter misidentification?

Craft responded in the affirmative to all three questions. The EAC is working on a federal certification program which will assume the role of the NASED voluntary accreditation program. Absentee ballots pose a high security threat even with stringent laws. Insider threats are an issue. You need to have effective management, separation of duties, and screening of workers to mitigate the threat.

Creelan addressed the voter misidentification issue. As distinguished from documented insider election fraud, voter fraud has not been shown to exist in great numbers. When you consider risk analyses, assumptions of individual voter fraud are somewhat baseless.

*Question/Comment:*An audience participant raised the issue to the panel of all-inclusive certification of voting systems to include the support materials for poll workers.

Jones indicated that he advocated that all voting systems include the support material needed to administer them. Vendors tend to be reluctant to tell the purchaser or examiner to guard against certain threats. He illustrated this point with an inadequate explanation for poll workers on calibrating the touch screen.

Selker agreed that system support information for poll workers needs to be at an understandable level for poll workers with limited education. He also indicated that the right qualification test for poll worker competency was not necessarily a written IQ type test but rather a performance test where the poll worker demonstrates their capability to carry out required tasks.

DeBeauvoir discussed the management issues surrounding those individuals who believe they are entitled to be poll workers but are not judged competent in dealing with the operation of new computerized voting equipment and election procedures.

Question/Comment: Coney posed several questions for the panel related to chain of custody of voting equipment, including the voter activation card. Coney commended the panel. She referred the panel to the state of Maryland's poll worker "debriefing" as a useful post-election feedback procedure for identifying new threats. Also, poll workers were sent a survey to fill out on their experiences both in training and on Election Day. This is a model worth emulating in other jurisdictions. An initial question for the panel concerned the role of privacy and transparency in making elections more secure. Are the processes intertwined within security issues? A second question dealt with security related to voter access and activation cards.

DeBeauvoir indicated that procedures need to be in place to account for all of the voter activation cards at the end of Election Day. You document the number of cards used and compare that figure with the number of voters. To the extent that you discover missing voter access cards, you so document that in writing and install procedures to prevent this from happening in future elections. Again, this is part of the continuous improvement cycle for security procedures.

Coney asked if these cards, when used in future elections, pose a security threat.

Selker noted that these "smart cards" are programmed uniquely for each election.

Rubin indicated that if an adversary obtains these preprogrammed voter access cards, it provides only minimal assistance in subverting a future election.

Craft emphasized that a prudent election administrator will re-key the security information on the smart cards and the voting machines between elections as standard operating procedure.

Shamos recognized this case as a simple example of an instance where there is a simple managerial defense already available. The threat here is that a voter will save an access card and correctly reprogram it as validated for the next election. The card would provide a means for the attacker to vote twice in the next election- once with this card and a second time with the new card provided by the clerk on Election Day. However, with proper election management procedures in place, a poll worker would routinely check the public counter on the DRE between voters. The poll worker could then easily determine if a voter has voted twice.

DeBeauvoir brought up the issue of plausibility of this attack. It would seem more plausible for a voter to register twice with two different addresses and then vote in two different locations rather than to spend the considerable effort to correctly revalidate a voter access card to allow them to vote twice.

Question/Comment: Klein requested the panel's reaction to the issue of attacker profiles including the amount of money available for attacks by the entire attacker community. He provided an estimate of .25 billion dollars in a four-year election cycle in his position paper (see: http://vote.nist.gov/threats/papers/threat-modeling.pdf). The asset being protected is "governmental power." These are issues that should be part of a threat analysis. Secondly, the current discussion is one of matching the technology to the capabilities of the poll workers and the election administration officials. Non-technologically oriented individuals are being asked to watch for sophisticated attacks on complex voting systems. He posed the solution of paper backed up by evidentiary quality chain of custody procedures.

Craft addressed the issue of "dumbing down" the technology to meet the poll worker's capability. This is not an option in an environment where the operating requirements for the voting equipment have increased every year. An election administrator has to find poll workers with the capability to carry out the required procedures for a secure election. This may require a petition to state legislators for increased pay and benefits to recruit suitable individuals (retirees, government workers, etc.) to address the supply and demand challenges.

DeBeauvoir added that you can also have job descriptions for poll workers that match their level of skill. An election administrator also can create a smaller group of trained trouble shooters who travel around supporting election judges by answering questions and repairing equipment.

Rivest agreed with Klein that it is a fair assumption that the attack community has a fair amount of financial resources. As a nation, we need to address the underfunded effort to deal with the attack threats with improved technology and quality management procedures.

Selker referred to the quarter billion dollar estimate as hypothetical. He questioned whether paper was any less fallible than other technologies to security threats.

Rubin addressed the adversary issue from the standpoint of the substantial incentive to do harm. That incentive is control of the free world.

Craft noted that the debate over voter verified paper trail versus DREs and other voting technologies is moot. Congress has left the decision to the states regarding appointment of delegates, which translates down to state control on how they will conduct elections. The arguments over the methods of elections will never be resolved because individual jurisdictions will make their own decisions. The task at hand is to determine best practice to mitigate risk for each of the voting technologies in use.

Creelan asked a series of related questions of the other panelists that required a broader view of the purpose of the "Threat Analysis for Voting Systems" workshop. What do we mean by threats? Are we limited to deliberate attacks or are we including other areas where things can go wrong? Are we privileging security at the expense of other values including accessibility, equality, and usability? Are we limiting our concerns to voting systems and not the entire voting process, including registration?

Craft believed that great pains have been taken in the workshop to apply the broadest definition of threats to the entire process. The threats we are addressing are those events- accidental and intentional- that can cause an election to come to a wrong result.

Question/Comment: An audience participant asked the panel to address changing the dates of elections to weekends or holidays. She also inquired about a cost analysis of the election process. There seems to be no analysis of the aggregate cost of an election including registration and hiring poll workers as well as equipment costs, etc., is there a cost analysis of high-tech voting methods (higher costs) versus low-tech methods (lower costs)?

Creelan indicated that the Brennan Center is working on determining those costs. The ultimate goal is to create a cost calculator where an election official can enter in variables particular to a jurisdiction. The output would be a range of costs for various systems. It is a complicated exercise. "Apples and oranges must be reconciled." Currently there is inadequate information to make available to the election administrator, and only incomplete conclusions can be drawn on election purchases.

Panel 3- Wrap Up, Conclusions, Next Steps

Donetta Davidson, Ray Martinez, Mark Skall, John Wack, Linda Lamone, Panel 1 members and Panel 2 members

Moderator: Barbara Guttman, NIST Information Technology Laboratory

The new panelists introduced themselves.

Donetta Davidson, EAC Commissioner
Ray Martinez, EAC Commissioner
Linda Lamone, Maryland State Director of Elections
Mark Skall, NIST, Information Technology Laboratory
John Wack, NIST, Information Technology Laboratory

Guttman introduced the goals of the final panel - to summarize where we have been and where we go from here.

Lamone expressed four summary points relating to consensus issues expressed at this workshop and an editorial comment. She thoroughly endorsed minimum quality assurance standards and guidelines for the manufacturers of voting equipment that include documentation standards. Secondly, election administrators in the field need guidelines, standards, and best practices for logic and accuracy tests, chain of custody, and parallel testing for all of the different types of voting equipment. Thirdly, the scientific and academic community needs to work closely with the elections administration community. Security-related problems will get solved only if we work together. Lastly, and most importantly, security discussions such as those at future workshops need to focus on existing voting systems. In order to be HAVA-compliant, election jurisdictions are making or have made purchase decisions. The 2005 voting standards proposed by the TGDC and adopted by the EAC will deal primarily with current technology. Election administrators need help making sure the voting systems they purchase are manageable and secure. Lamone offered an editorial comment that the failure rate in Maryland in the 2004 election was less than 1 percent, contrary to what some advocates say.

Skall summarized what he hoped NIST and the TGDC would take away from this workshop. Looking at our goals for this workshop, we identified many of the threats as plausible. There is clearly still much work to be accomplished in the area of threat analyses of election systems. A successful end result would be future security requirements proposed by the TGDC and delivered to the EAC that are traceable back to specific threats. Cost to the states to adhere to these requirements could be substantial. Quantification of threats represents a difficult task. We might look at this as “expected value” or “expected damage,” which would be the probability of a threat times the actual dollar value of the damage. If we could determine this value, we could give more guidance to the TGDC as to how much time to spend on requirements that address specific threats.

Commissioner Davidson thanked NIST for starting the process of addressing the issues of voting system security in terms of threat analyses. Activities we are undertaking at the EAC will assist election administrators with management issues raised at this workshop. We have a number of

studies underway to determine best practices for election administration at the state and local levels. EAC will be working with NASED on management guidelines. As we have heard at this workshop, training is part of the risk assessment process. When considering resources to deal with threats, it is important to include small and medium-sized counties and jurisdictions in the analysis. As well as money, technology resources represent a challenge to smaller municipalities. This workshop represents a good start and provides the voters with trust and confidence that we are addressing the security issues critical to fair and safe elections.

Commissioner Martinez expressed his gratitude for the large turnout for this productive workshop, especially the discussion of the threats to voting systems in general. The EAC is striving to make progress in the area of election administration. HAVA was meant to improve the three-legged stool of election administration- the technology we use, the processes in place to ensure fairness at the polling place on Election Day, and the people involved in running the election. With HAVA, Congress appropriated $3.1 billion to improve all three aspects of election administration- the technology, the processes, and the people. An example is that jurisdictions are using the money to switch from lever machines and punch cards to op scan or DRE technologies. With respect to processes, HAVA also requires states to look at their election codes and to better define what "the intent of the voter" means. Finally, HAVA dollars are intended to help ensure that election officials and poll workers have the training to do the job correctly. In a December 2004 Wall Street Journal poll with a sample size of one thousand, 24 percent of those polled indicated they had little to no confidence that the vote they had cast had been correctly recorded. While the Commissioner is certain that election administrators are working diligently to ensure the integrity of the elections, we cannot deny the issue of lack of voter trust, and we must deal with it. Jones pointed out in his paper (see : http://vote.nist.gov/threats/papers/threats_to_voting_systems.pdf) that we need to solve this problem voluntarily before Congress or state regulatory bodies decide to solve it for us (i.e., a regulatory scheme is mandated). The Commissioner stated that he believed a voluntary cooperative effort to improve voter confidence is preferable to a regulatory scheme. This requires frank and earnest discussions in areas such as security threats to voting systems. It also requires pulling together best practice tools for state and local election administrators so that they can improve the election management process. Innovation is critical to improving trust and confidence of the voters.

Rivest addressed the issue of determining the probability of various attacks. If you think about any system from an attacker's point of view, you will try to go through "the open door" and not "the closed window." Cryptography succeeds when it is no longer the weakest link. If you have a voting system with many components and resultant vulnerabilities, there will be many different attacks you can employ. You cannot determine the probability of an individual attack any more than you can determine the probability of someone choosing a particular window or door, regardless of whether it is open or closed. It is a large-scale contextual problem. The right questions to ask are, 'What is the difficulty of achieving a particular attack?' and 'Where is the weakest link' in the entire system?" That is where the probability will be highest. Voting is interdisciplinary and requires input from people involved in every part of the election process to make it work better. We should have conferences like this devoted to analyses of voting threats.

Jones returned to the subject of a cost-benefit analysis of voting threats. Economic analysis of security is inherently difficult because you are spending money to avoid risk. Your most successful purchase with security is one where you never notice the benefit because you do not

see an attack. You have spent the money well because you have deterred the threat. Therefore, economic analysis of risk produces almost bogus numbers. Sometimes money spent by management produces defenses against threats that were not even anticipated. The Y2K spending is an example of one such threat which put into place necessary redundancies to survive the anthrax attack. Jones also commented on the previous discussion of the "omniscient hacker." Looking back at Harris' 1934 analysis of threats to elections (see: http://vote.nist.gov/election_admin.htm), the hot topic for threats then was mechanical lever machines. There was a push to replace paper voting machines with paperless mechanical lever systems because they were allegedly more resistant to fraud. By the 1950s, the fraud possibilities were quite clear; mechanical voting machines could be and were in fact rigged long before it came to public notice. Thus, we cannot take the risk of claiming that we have the exhaustive threat catalog. While the vast majority of election jurisdictions have lived up to high standards, a minority have not done so.

Shamos agreed that no threat should be dismissed out of hand. Every threat deserves serious consideration even if the response is that we consider it unlikely to occur. The way to do this is to continue assembly of the threat catalog. Then it makes sense to develop standards (requirements) and cross-references from the standards to the threat catalog. When we find a threat that is not addressed by a corresponding standard, we have a wake-up call to address a risk that has not been covered.

Wack addressed the job of NIST and the TGDC to produce recommendations for future iterations of the VVSG. Several points discussed at this workshop will assist in this effort. Participants expressed a need for more documentation with respect to voting systems and procedures for poll workers. Voting systems can be much more secure if they are simpler. Voting system design is critical, especially with respect to usability by the poll worker as well as the voter. With respect to independent dual verification, more developmental research is necessary.

Skall agreed that many of the large economic studies are not useful and fail to provide the needed insight. On the other hand, even if we have specific requirements to address each threat in a threat catalog, there is no guarantee that the requirement will be precise or testable. You need to drill down these requirements until you have completely addressed the issues of testability and precision. NIST and the TGDC need some sense of priority of each of these threats to see which are the most important and where we should dedicate most of our time and resources. There has to be some quantitative analyses, rough as it may be, to arrive at a prioritization that gives direction to NIST and the TGDC.

Rivest referenced the Brennan Center approach described earlier by Lazarus as a useful first-cut metric. This threat analysis looks at the number of people required to carry out an attack. If you have a threat where one person can take away 1 percent of the vote, you have a serious attack that requires mitigation.

Wack noted that a number of speakers pointed out that a number of security problems are in fact usability-related problems. From a prioritization standpoint, we may want to determine what "user error" problems we can fix now.

Commissioner Davidson agreed here that we need to split off the technically challenging problems from the user-error problems that can be worked on up front. In some instances, different groups can deal with the different issues.

Jones expressed concern here about "too much dividing," because it really is the case that every usability problem seems to be something that can be exploited in order to tinker with the vote. For example, if you can make things more usable in precinct 15 than they are in precinct 5, then you can effectively discriminate against the voters in precinct 5. That kind of strategy makes it possible to exploit almost every usability problem as a way to manipulate the election. That is why there needs to be a real cross connection between the voting systems standards and the best practices guidelines. Jones believes that, in many cases, the technology standards we have make assumptions about the ways the users are expected to use that technology. We need procedural documentation here. The voting system standards assume poll worker procedure standards.

Panel 3 Audience Participation:

*Question/Comment:*An audience participant asked the EAC Commissioners to address the roll of the EAC in updating the certification process when new vulnerabilities are discovered. Will the independent testing authorities (ITAs) at the state and federal levels receive feedback to update the voting system tests when new threats or vulnerabilities are discovered? Will the EAC oversee this certification review process?

Commissioner Martinez answered yes. There is some debate here concerning the role of the EAC. However, Congress has given the EAC the responsibility of becoming the certifiers of voting systems at the national level. The EAC is obligated under HAVA to transition from the NASED certification program to one administered by the EAC. We are still in the process of putting together the transition program and hope to have it in place in the next six months. We have a responsibility in the new certification program to keep track of patterns that would signal that a particular voting system has a particular vulnerability and to transmit that vulnerability to jurisdictions across the country, the ITAs, NIST, and the TGDC to address these kinds of problems.

*Question/Comment:*Lewis thanked NIST for holding this workshop on the security of voting systems. He made the point that perspective is important when assessing surveys of the confidence of voters in the perception of whether their vote was accurately recorded. In fact, surveys of voter trust have never been higher than 88 percent. He asked the panel whether he thought that Congress was committed to give NIST and the EAC what they need to improve voting systems.

Commissioner Davidson answered that, at least for FY 2006, Congress has funded the EAC at the same level as FY 2005. Beyond that, it is difficult to say.

*Question/Comment:*McClure asked the panel to address state statutes and their differing requirements with respect to electronic voting systems as well as the sometimes-conflicting relationship of state standards to federal standards.

Shamos noted that states began holding independent hearings in the mid 1980s to address these issues. Today, the electronic voting statutes in almost every state are quite detailed. They make

careful distinctions between paper-based, lever systems and electronic systems. There are conflicts that states such as Pennsylvania have had to address with respect to interpretation by the vendors.

Commissioner Martinez addressed the issue of determining an effective date for the new voluntary voting system guidelines. In trying to determine this date, the EAC looked at state election codes and found that there was problematic wording that would play into any effective date the EAC chose. The EAC is taking into consideration how state laws and administrative procedures deal with decisions made at the federal level.

Question/Comment: Klein gave credit to the state of Maryland for conducting the first penetration tests of voting systems. However, that test was not comprehensive and did not rise to the level of a systematic search for vulnerability of critical systems that is included in documents such as the common criteria. In his comments on the VVSG, Klein notes that the lack of such penetration testing basically negates most of the security improvements. Serious security testing needs to be part of any program that goes forward.

Rivest agreed that a test of open-ended vulnerabilities is important in any security review. The TGDC has passed a resolution authorizing NIST to develop standards in that direction. Those are not part of the current VVSG because we had to prioritize NIST's work in a limited time frame to produce the current version. Rivest hopes to see future development of these standards.

Appendix

Threat Analyses Submitted as of 10/7/05

1. **Chain Voting** - Douglas W. Jones

2. **Spooled Paper** - John Wack

3. **Optical Scan Configuration File** - Douglas W. Jones
   - **Comment by Steven Freeman**

4. **Optical Scan Ballot Design** - Douglas W. Jones

5. **Incompetent Poll workers** - Douglas W. Jones

6. **Security Risks Associated with Pre-election Delivery of Electronic Voting Machines** - Barbara Simons

7. **Touch Screen Calibration** - Douglas W. Jones

8. **Optical Scan Calibration** - Douglas W. Jones

9. **Touch Screen Window Manager** - Douglas W. Jones

10. **Exploitation of Compromising Electromagnetic Emanations** - Stanley A. Klein

11. **Smartcard Port Attack** - Stanley A. Klein

12. **Misprogramming Threat** - Jeremy Epstein

13. **Wi-Fi Usage in Voting (without inside assistance)** - Jeremy Epstein

14. **Wi-Fi Usage in Voting (with vendor complicity)** - Jeremy Epstein
    - **Response to WiFi Usage** - James C. Johnson

15. **Voter "Assistance"** - Douglas W. Jones

16. **VVPR Attack with Misprinted VVPAT** - David L. Dill

17. **Trojan Horse in DRE Application Software** - Stephen Green

18. **Replaceable Media on Optical Scan** - Harri Hurst

19. **Trojan Horse In Tally Server** - Chris Lowe

20. **Attack on Configuration Data** - Eric Lazarus/Stephen Green

21. **Ballot Marking Device Attack** - Eric Lazarus
22. **Trojan Horse in DRE - OS** - Chris Lowe

23. **Paper Trail Boycott** - Michael Shamos

24. **Paper Trail Manipulation** - Michael Shamos

25. **Paper Trail Manipulation (2)** - Michael Shamos

26. **Cellphone Vote-Buying** - Michael Shamos

27. **Security Vulnerabilities and Problems with VVPT** - Ted Selker and Jon Goler

28. **Denial of Service (Bottleneck)** - Robert Fleischer

29. **Precinct Voting Denial of Service** - R. Michael Alvarez

30. **Potential Threats to Statewide Voter Registration Systems** - R. Michael Alvarez

31. **Malware Loader** - Ron Crane

Related Papers Submitted at of 10/7/05

1. **Minimum Security Procedures for Voting Systems**

2. **Response by the Florida State Association of Supervisors of Elections**

3. **Threats to Voting Systems** - Douglas W. Jones

4. **Voting System Threat Modeling** - Stanley A. Klein

5. **Method for Developing Security Procedures in a DRE Environment** - Dana DeBeauvoir

6. **Voting Resolution** - Brevard Democratic Executive Committee

7. **Strategies for Software Attacks on Voting Machines** - John Kelsey

8. **All Threats** - David Biddulph

9. **Software IS a Problem** - Bob Fleischer

10. **Comment**-The Information Technology Association of America's (ITAA) Election Technology Council